Videosicherheitstechnik

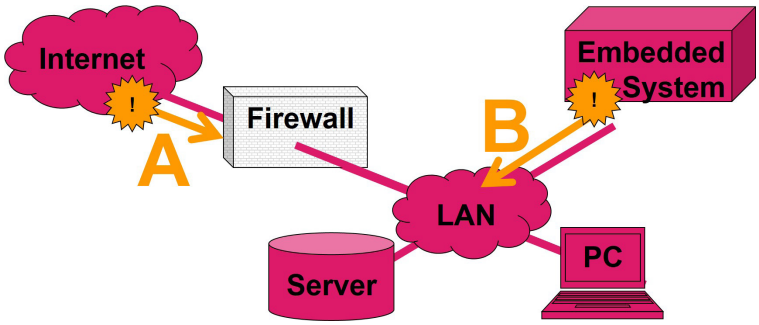
Cyber Security bei Videoanlagen

Wichtige Hinweise für Errichter

Digitalisierung und Vernetzung verändern auch die Videosicherheitstechnik grundlegend: Klassische analoge Videokameras mit direkt zugeordneten (dedizierten) Videoaufzeichnungsgeräten (Recordern) werden ersetzt durch immer leistungsfähigere IP-Kameras, die in einer komplexen IT-Infrastruktur betrieben werden. Damit wachsen auch die Herausforderungen, die für einen sicheren Betrieb dieser Anlagen zu meistern sind.

Das Thema Sicherheit wird meist intuitiv mit Angriffen von außen in Verbindung gebracht. Folgerichtig unterliegen bei den üblichen Firewall-Einstellungen vor allem jene Verbindungen strengen Regeln, die von außen (aus dem Internet) nach innen (in das private Netz, LAN) aufgebaut werden.

Hingegen wird der Aufbau von Verbindungen von innen nach außen meist nicht oder nur wenig reglementiert, um den Zugriff der Anwender auf die verschiedenen weltweiten Internet-Anwendungen und Dienste nicht zu beeinträchtigen.



Netze sind oft nur gegen Angriffe von **außen (A)** geschützt. Die Erfahrung zeigt jedoch, dass Angriffe auch von **innen (B)** erfolgen. Viele Videoanlagen sind dagegen unzureichend geschützt. Statt zu mehr Sicherheit führen solche Anlagen zu mehr Risiko.

Hier besteht dringender Handlungsbedarf für Errichter und Betreiber!

Unterschätztes Risiko „Embedded Systems“

Embedded Systems (eingebettete Systeme) sind Computer, die für einen bestimmten technischen Zweck in ein Gerät eingebaut werden und dort – für den Anwender oft unsichtbar – ihren Dienst tun.

Mit Produkten aus dem Smart-Home-Bereich, „intelligenten“ Lautsprechern, Alarmanlagen und auch IP-Kameras halten sie Einzug in viele private Netze, ohne dass den Anwendern die damit verbundenen Gefahren bewusst sind.

Embedded Systems birgen Risiken, weil sie durch die Firewall von innen nach außen Verbindungen aufbauen können. Ist eine solche Verbindung erst einmal hergestellt, können Angreifer darüber das Gerät steuern und somit das private Netz (LAN) von innen angreifen.

Server und PCs sind als sicherheitsrelevante Technik klar zu erkennen und werden entsprechend sorgfältig in Sicherheitskonzepten berücksichtigt. Risiken, die von eingebetteten Systemen ausgehen, werden dagegen häufig unterschätzt, weil bei diesen Geräten die Hauptfunktion im Mittelpunkt steht und nicht auf den ersten Blick zu erkennen ist, was alles im Gehäuse steckt. Eine IP-Kamera ist aber eben nicht nur eine Kamera, sondern ein voll vernetzter Computer mit allen Möglichkeiten und Risiken, die diese komplexe Technik bietet.

Bei Entwicklung und Auswahl von embedded Systems stehen meist Funktion und Preis im Vordergrund. Das hat zur Folge, dass die Datensicherheit oft vernachlässigt wird.

Viele embedded Systems bauen bereits ab Werk automatisch Verbindungen zu externen Servern auf, etwa für Updates, Fernwartung oder zum Speichern von Daten in der „Cloud". Diese Verbindungen unterlaufen die Firewall; der Anwender hat in der Regel keine Kontrolle darüber, welche Daten über diese Verbindungen transportiert werden. Bei manchen Geräten sind Hintertüren bekannt geworden, die versehentlich oder absichtlich eingebaut wurden. Mitunter werden Geräte auch gezielt von Geheimdiensten, Industriespionen oder der organisierten Kriminalität manipuliert. Solche kompromittierten Systeme stellen ein erhebliches Sicherheitsrisiko für das gesamte betroffene Netzwerk und Unternehmen dar.

Mögliche Ursachen für Angriffe von innen:

- Von Anwendern eingebrachte Schadsoftware / Plugins
- Backdoors der Hersteller, z.B. für Support, Behörden, …
- Sicherheitslücken (fehlende Updates, Standard-Passworte)
- Verbindungen für Updates, Video-Hosting, Fernwartung, …
- für Spionagezwecke präparierte Geräte
- u.v.m.

Dieses Risiko ist nicht abstrakt und theoretisch, sondern ganz konkret und hat in der Praxis bereits zu erheblichem wirtschaftlichen Schaden geführt. Das zeigen folgende Beispiele:

- Eine russische Hackergruppe hat im Zuge der Kampagne „Carbanak" u.a. Überwachungskameras in Banken kompromittiert und konnte Millionenbeträge erbeuten.
- Die Schadsoftware „Mirai" hat u.a. zahlreiche Überwachungskameras für einen DDoS-Angriff genutzt.
- Überwachungskameras des amerikanischen Herstellers „NetBotz" waren jahrelang mit einer Hintertür in vielen Unternehmen und kritischen Bereichen eingesetzt, u.a. in Serverräumen.

Auch aus Gründen der Informationssicherheit und des Datenschutzes müssen Errichter und Betreiber von Videosicherheitssystemen sicherstellen, dass nur berechtigte Nutzer auf die Geräte und Daten zugreifen können.

Herausforderung IP

Für klassische Videoüberwachungsanlagen hat sich die Abkürzung „CCTV" etabliert. Das CC steht für „Closed Circuit". Damit ist gemeint, dass nur ein geschlossener Benutzerkreis auf diese Anlage und ihre Daten zugreifen kann. Mit der Umstellung auf IP ist grundsätzlich ein weltweiter Zugriff möglich. Deshalb muss durch geeignete technische Vorkehrungen dafür gesorgt werden, dass auch IP-basierte Videoanlagen wieder zu geschlossenen Systemen werden.

Während Anwender von ihrem IT-Endgerät (PC, Smartphone) weltweit uneingeschränkten Zugriff auf alle Anwendungen und Dienste wünschen, sollen bei Video Sicherheits Systemen (VSS) die Bilder einer begrenzten Anzahl Kameras nur auf einer wohldefinierten Auswahl von Monitoren dargestellt werden. VSS erlauben und erfordern deshalb engere Regeln als allgemeine IT-Systeme.

Die **oberste Sicherheitsregel** lautet: Das Netzwerk darf ausschließlich nur die explizit gewünschten Verbindungen zulassen; dann können embedded Systeme keine Verbindung zu einem Angreifer aufbauen.

Das Risiko unerwünschter Verbindungen lässt sich durch geeignete technische Vorkehrungen vermeiden. Die so gewonnene Sicherheit rechtfertigt den größeren Aufwand und die höheren Kosten. Zumal die ohne Vorkehrungen zu befürchtenden Schäden sehr viel höher wären.

Der Sicherheit stehen oft entgegen

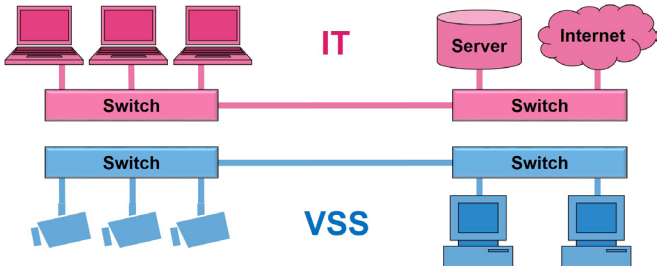
- Bequemlichkeit
- mangelnde Kenntnisse
- Kosten sparen „um jeden Preis"

Von Vorteil ist, bereits bei der Planung einer Videoanlage ein passendes Sicherheitskonzept zu wählen. Wir zeigen verschiedene Lösungsalternativen in der Reihenfolge von „ganz sicher" bis „voll vernetzt", die je nach gegebener Aufgabenstellung auch miteinander kombiniert werden können.

Lösungsalternativen

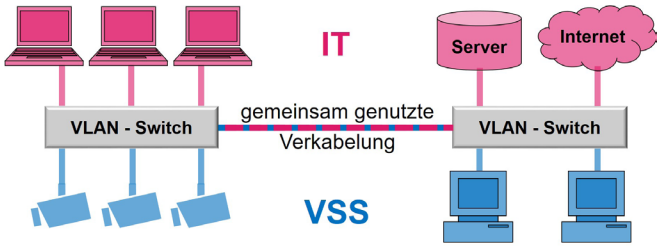
1. Einfach und sicher – separate Netze

Ein separates Netz für Video bringt die größte Sicherheit und wird deshalb vom BHE empfohlen.
Die physikalische Trennung der Leitungen kann von keiner Software überwunden werden. Höhere Kosten oder fehlende Kabeltrassen zwingen aber oft dazu, Video über vorhandene Kabel zu transportieren.



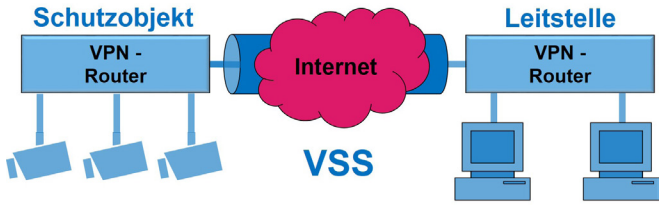
2. Mehrere Netze auf einem Kabel – VLAN

Mit einem Virtual Local Area Network (VLAN) kann vorhandene Verkabelung genutzt werden, um darauf mehrere logisch getrennte Netze zu realisieren. Dies erfordert durchgängig VLAN-fähige aktive Netzwerkkomponenten (statisches oder tagged VLAN nach IEEE 802.1Q) und eine konsequente fachgerechte Konfiguration.



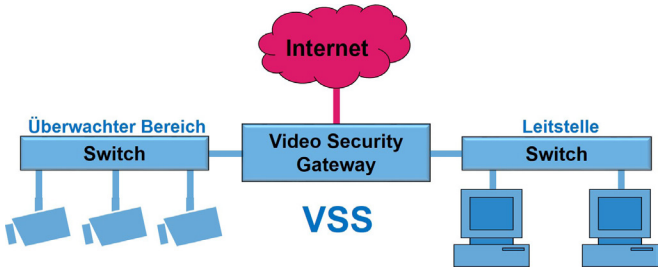
3. Ein sicherer Tunnel für Daten auf ihrem Weg durch das Internet – VPN

VPN ist das Mittel der Wahl wenn sensible Daten über das Internet übertragen werden sollen.
Es ist darauf zu achten, dass alle Videodaten stets im LAN, VLAN und VPN verbleiben. Alle internen und externen Verbindungen außerhalb dieser geschützten Bereiche sind zu unterbinden.



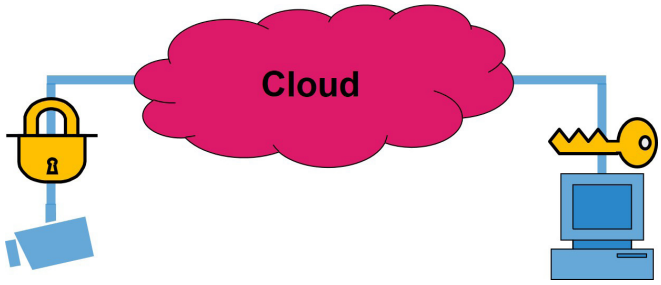
4. Sichere Verbindung nach außen – Video Security Gateway

Wenn doch Verbindungen zu anderen Netzen benötigt werden, sollten diese durch einen speziellen Netzwerkübergang (Gateway) geschützt werden.
Ein Video Security Gateway überwacht alle ein- und ausgehenden Verbindungen und kombiniert dabei verschiedene Sicherheitsmaßnahmen, die speziell auf die Belange der Videosicherheitstechnik abgestimmt werden.



5. Konsequente Verschlüsselung für alle vertraulichen Videodaten

Eine durchgängige„Ende-zu-Ende-Verschlüsselung“ von der Kamera bis zum Monitor gewährleistet, dass niemand unbefugt auf die Videodaten zugreifen kann.
Dies ist insbesondere dann geboten, wenn Videodaten z.B. in der„Cloud“ gespeichert werden sollen. Entscheidend: Wer besitzt den Schlüssel?



Video-Security-Gateway

Wichtig ist bei allen Lösungen, dass auf mögliche **Netzwerkkopplungen** geachtet wird: Alle Geräte, die an mehrere Netze angeschlossen sind, können (ggf. auch ungewollt) Verbindungen zwischen diesen Netzen herstellen. Deshalb dürfen alle Geräte jeweils nur an 1 Netz angeschlossen werden. Sind weitere Kommunikationsbeziehungen nötig, so dürfen diese nur über ein Security Gateway erfolgen.

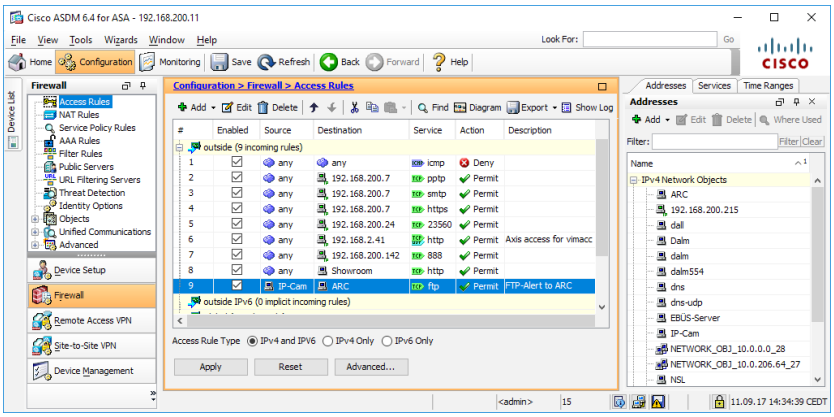
Ein Video-Security-Gateway enthält u.a. folgende Sicherheitsfunktionen:

- **Firewall**: Lässt nur explizit gewünschte Verbindungen zu
- **Router**: Stellt nach vorgegebenen Regeln Verbindungen her
- **NAT**: Verbirgt die IP-Adressen des internen Netzes
- **DMZ**: Pufferzone zwischen äußerem und innerem Netz
- **Protokollanalyse**: Verdächtigen Datenverkehr erkennen
- **Virenscanner**: Prüft alle Daten auf verdächtige Strukturen

Firewall

An der Firewall sollten zunächst alle ein- und ausgehenden Verbindungen gesperrt werden. Dann werden gezielt ausschließlich nur die explizit vom Kunden gewünschten und benötigten Verbindungen freigegeben. Diese **Whitelist** sollte regelmäßig geprüft und nicht mehr benötigte Einträge entfernt werden.

Welche Sicherheitseinstellungen eine Firewall bietet und wie diese konfiguriert werden, hängt vom jeweiligen Hersteller und Produkt ab. Neben fundierten Kenntnissen über digitale Netze ist deshalb auch eine Schulung speziell zu den verwendeten Produkten nötig, damit ein Errichter seine Arbeit ordnungsgemäß ausführen kann.

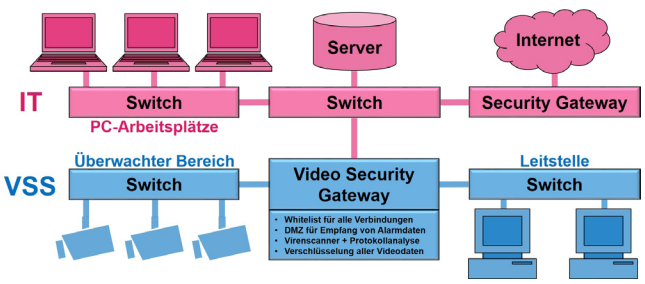


Firewall Konfiguration am Beispiel Cisco ASDM

Wichtig ist ein **ganzheitlicher Ansatz**: Auch wenn die Videoübertragung z.B. nur für TCP/IPv4 ausgelegt ist, könnte Schadsoftware auch IPv6, ICMP, DNS oder den UDP-Protokollstack nutzen. Schadsoftware zweckentfremdet gern Standardports und unverdächtige Protokolle. Da sie nur spontan aktiv wird, muss das Gateway dauerhaft alle Verbindungen überwachen, nicht nur die vom VSS genutzten.

Videonetz im Kundennetz – Kaskadierter Schutz

Die strengen Sicherheitsregeln des VSS können möglicherweise nicht an der beim Kunden bereits vorhandenen Firewall umgesetzt werden, weil dort noch anderer Datenverkehr fließt, der flexibler gehandhabt werden muss.
Lösung: Zweites Security Gateway zwischen Kunden-LAN und Video-LAN



Videomanagementsysteme (VMS) und Verknüpfung mit anderen Sicherheitsgewerken

Besondere Aufmerksamkeit und Fachkompetenz ist erforderlich, wenn Videoanlagen mit Videomanagementsystemen geplant sind – insbesondere auch dann, wenn diese u.U. auch eine Verknüpfung mit anderen Gewerken wie etwa Zutrittskontrolle, Intercom, Gebäudeleittechnik, BMA, EMA zulassen oder in Building-Managementsystemen oder einer komplexen IT-Infrastruktur integriert werden sollen.

Aus Sicherheitsgründen sollten alle Gewerke und ihre Netze sauber voneinander getrennt bleiben. Große Netze sollten in separate Teilnetze aufgeteilt werden (subnetting), und zwischen diesen Teilnetzen sollten gezielt nur die erwünschten Verbindungen zugelassen werden, damit beispielsweise sensible Unternehmensdaten vor Zugriffen aus dem Videosystem geschützt bleiben.

Die Verbindung zwischen diesen Netzen erfolgt ausschließlich über Security Gateways, in denen die Router-Funktion (Vermittlung der Datenpakete zwischen den verschiedenen Netzen) mit angemessenen Sicherheitsfunktionen wie z.B. FireWall, NAT, VLAN, Virenscanner u.s.w. in einem Gerät kombiniert sind.

Solides und aktuelles Fachwissen gefordert

Planung, Konfiguration und Administration derart komplexer Netze und der dazu nötigen aktiven Netzwerkkomponenten erfordern solides und aktuelles Fachwissen auf diesem Gebiet, damit nicht durch Unkenntnis Sicherheitslücken entstehen.

Auswahl des passenden Lösungsansatzes

Welche Lösung für welchen Anwendungsfall optimal ist, hängt von den Anforderungen und Randbedingungen der jeweiligen Projekte ab. Einige Beispiele sollen dies verdeutlichen:

- Wenn die Entfernungen zwischen Kameras und Monitoren nicht zu groß und geeignete Kabeltrassen frei zugänglich sind, ist die Einrichtung eines separaten Videonetzes die einfachste, sicherste und auch kostengünstigste Lösung.
- Wenn auf bestimmten Strecken eine eventuell bereits vorhandene IP-Verkabelung mitgenutzt werden soll, bietet sich VLAN als Lösung an.
- Für den Fernzugriff auf Videobilder durch das Internet stellt VPN die passende Lösung dar.
- Werden weitere Verbindungen benötigt (etwa zu einem Management-System) oder soll das Videosystem in ein Kundennetz integriert werden, sollte ein Video-Security-Gateway zwischengeschaltet werden.
- Sollen vertrauliche Videodaten im Internet übertragen oder gespeichert werden (z.B. bei „Cloud-Lösungen"), ist eine zuverlässige durchgehende Verschlüsselung geboten.

Kein Formalismus kann ersetzen, dass Planer und Errichter von Fall zu Fall sorgfältig abwägen, wie die jeweiligen Anforderungen des Kunden am besten umgesetzt werden können, denn hier spielen noch eine Fülle weiterer Parameter eine Rolle. Fachkundigen Rat bietet bspw. der BHE.

Feste IP-Adressen verwenden

Um variable (dynamische) IP-Adressen nutzen zu können, wird ein Domain Name System (DNS) benötigt. Dieses ist jedoch angreifbar (z.B. mit DDoS). Manipulierte DNS-Einträge können Verbindungen zu ungewollten Gegenstellen bewirken. Nach der täglichen Zwangstrennung und Neuzuweisung einer dynamischen IP-Adresse ist eine Aktualisierung der DNS-Einträge notwendig. Während dieses Vorgangs, der mehrere Minuten dauern kann, ist keine Verbindung möglich.

Dynamische IP-Adressen sind deshalb nicht für sicherheitsrelevante Anwendungen geeignet!

Authentifizierung

Es muss damit gerechnet werden, dass Angreifer und Schadsoftware die Standard-Passwörter (default passwords) vieler Produkte kennen, denn Listen dieser Passwörter sind im Internet frei zugänglich. Unmittelbar bei der Erstinbetriebnahme müssen deshalb auf jedem Gerät eigene „starke" Passwörter konfiguriert und die vom Hersteller vorkonfigurierten Benutzerkonten gelöscht werden.

Hersteller sollten verhindern, dass ihre Produkte mit Standard-Passwörtern im Wirkbetrieb genutzt werden, etwa durch wiederholte Hinweise und indem die Gültigkeit der initialen Zugangsdaten begrenzt wird.

Bild: Maksim Kabakou / iStock / Thinkstock

Vom BSI empfohlene Maßnahmen

Das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) empfiehlt in seinem Dokument [2] „Sicherheit von IP-basierten Überwachungskameras“ (Version 1.10 vom 08.11.2016) die folgenden Maßnahmen (die kurzen Erläuterungen und Kommentare dienen der besseren Verständlichkeit):

- **Ungeschützte Erreichbarkeit über das Internet vermeiden**
  ⇨ durch Firewall und NAT-Router wie bei „Video Security Gateway“ beschrieben
- **Ausgehende Kommunikation durch Firewall einschränken**
  ⇨ s. „oberste Sicherheitsregel“ auf S. 2 und ff in diesem Informationspapier
- **Selbstgewählte hinreichend starke Passwörter verwenden**
  ⇨ s. Abschnitt „Authentifizierung“
- **Fernzugriff nur über VPN ermöglichen**
  ⇨ s. Lösungsalternative 3 auf S. 3
- **Nur benötigte Dienste aktivieren**
  ⇨ Jeder aktive Dienst stellt ein mögliches Risiko dar. Deshalb sollten alle nicht benötigten Funktionen und Komponenten abgeschaltet bzw. gesperrt werden.
- **Nur verschlüsselt kommunizieren**
  ⇨ s. Lösungsalternative 5
- **Beachtung des EOS Zeitraums**
  ⇨ s. Abschnitt „Neue Herausforderungen“
- **Einsatz ausreichend starker Authentisierungsmechanismen**
  ⇨ s. Abschnitt „Authentifizierung“ in diesem Informationspapier
- **Netzwerkseparation einsetzen**
  ⇨ s. Lösungsalternative 1 – 3 und Abschnitt „Netzwerkkopplung“
- **Zeitnahes Einspielen von Updates**
  ⇨ Papier „BHE-Empfehlungen zur Verwendung von Updates bei Videoüberwachungsanlagen“ [8] beachten:
  - Updates nur zu definierten Wartungszeiten einspielen, damit der Wirkbetrieb des Videosicherheitssystems nicht durch spontane automatische Updates gestört wird.
  - Updates können auch Fehler, Probleme und Risiken mit sich bringen. Deshalb alle Updates vor dem Ausrollen in den Wirkbetrieb erst auf einzelnen Systemen testen.
- **Monitoring der Kommunikation (Logfiles)**
  ⇨ Alle sicherheitsrelevanten Vorkommnisse, die beispielsweise von der Firewall erkannt werden, sollten protokolliert werden. Diese Logfiles sollten regelmäßig zeitnah vom Systembetreuer ausgewertet werden, damit Bedrohungen rechtzeitig erkannt und geeignete Maßnahmen umgesetzt werden können.
- **Cloud-Konzepte vermeiden**
  ⇨ s. Interview „Video in der Cloud“ mit M. Meissner, Vorsitzender BHE-Fachausschuss Video, www.bhe-videoueberwachung.de/cloud
- **Wi-Fi/WLAN in kritischen Bereichen vermeiden**
  ⇨ Gerade aktuell werden neue Sicherheitsprobleme bei WLAN erkennbar
- **Optionale Verwendung von Rechte- und Rollenkonzepte**
  ⇨ Jeder Anwender sollte nur genau die Rechte am System bekommen, die er zum Erfüllen seiner Aufgaben benötigt. Durch Zuordnung aller Aufgaben zu bestimmten Rollen und Zugehörigkeit jedes Anwenders zu den entsprechenden Gruppen kann dies übersichtlich und transparent implementiert werden.
- **Optional Verwendung physikalischer Zugriffsschutz**
  ⇨ Wenn etwa für IP-Kameras Netzwerkanschlüsse im Außenbereich verlegt werden, besteht die Gefahr von ungewünschten Zugriffen auf das Netz, sofern diese Zugänge nicht ausreichend mechanisch geschützt sind.

Achtung: Haftungsrisiko für den Errichter

Wenn Errichter bei ihren Projekten den anerkannten Stand der Technik nicht kennen bzw. nicht anwenden, gehen sie möglicherweise ein erhebliches Haftungsrisiko ein, falls ihre Kunden durch die von ihm installierte Technik Schaden erleiden.

Als „anerkannter Stand der Technik" können beispielsweise die Empfehlungen des BSI gelten.

Möglicherweise können in einzelnen Projekten nicht alle empfohlenen Sicherheitsmaßnahmen umgesetzt werden. Dies sollte dann mit den Kunden detailliert besprochen und die Kunden sorgfältig beraten werden. Außerdem sollten sich die Errichter ggf. schriftlich bestätigen lassen, wenn der Kunde beispielsweise aus Kostengründen bewusst auf bestimmte Schutzmaßnahmen verzichtet.

Bitte beachten Sie, dass auch der Eingriff in fremde Netze mit ernstzunehmenden Risiken behaftet ist. Errichter und Betreiber sollten Klarheit darüber schaffen, welche vertraglichen Pflichten bestehen und welche weiteren Bedingungen (technisch und gesetzlich) das Vertragsverhältnis betreffen. Weiterführende Informationen enthält das BHE-Papier „Haftungsrisiken bei der Integration von Sicherheitstechnik in kundeneigene Netzwerke - Schwerpunkt Videosicherheit". BHE-Mitgliedsunternehmen finden dieses im internen Mitgliederbereich unter www.bhe.de/de/FA-VUET-Uebersicht.

Bild: giampieroortenzi / iStock / Thinkstock

Mehrwertschöpfung durch den Errichter

In vielen höherwertigen Switchen und Routern sind Funktionen wie VLAN, VPN und Firewalls bereits enthalten und müssen nur geeignet konfiguriert werden.

Die spezifische Qualifikation des Errichters in Fragen der Cyber Security bedeutet somit einen erheblichen Mehrwert für den Kunden und eröffnet dem Errichter zusätzliche Geschäftspotenziale.

Aufschaltung von Videosystemen auf Leitstellen

Videokameras bringen nur dann einen Sicherheitsgewinn, wenn auf alle relevanten Ereignisse schnell reagiert wird. Deshalb ist die Aufschaltung von Videosicherheitssystemen auf rund um die Uhr besetzte, professionelle Leitstellen ein wichtiger Zusatznutzen, den Errichter ihren Kunden anbieten können.

Mit diesem Thema beschäftigt sich auch das BHE-Papier „Notruf- und Service-Leitstellen (NSL): Gute Gründe für eine Videoaufschaltung" .

Die Vernetzung mit Leitstellen stellt besondere Ansprüche an die IT-Sicherheit. Wichtig ist deshalb eine enge Zusammenarbeit zwischen Errichter und Leitstelle.

Neue Herausforderungen

Die Technik entwickelt sich rasant weiter, die Angreifer wenden immer raffiniertere Methoden an. Auf diese Weise entstehen neue Bedrohungen, auf die reagiert werden muss.

Moderne Videoanlagen sind komplexe IT-Systeme, die für einen sicheren Betrieb eine kontinuierliche fachgerechte Wartung erfordern. Dazu gehört, dass sämtliche Systemkomponenten regelmäßig mit Updates auf den neuesten Stand gebracht werden.

Errichter sollten deshalb vor Auswahl und Einsatz aller Systemkomponenten (PCs, Software, Router, IP-Kameras, …) klären, ob und wie lange der jeweilige Hersteller Softwarepflege für seine Produkte gewährleistet, in deren Rahmen auch alle neu erkannten Sicherheitslücken geschlossen werden (EOS Zeitraum wie in [2] beschrieben).

In Zukunft ist mit weiteren, neuartigen Bedrohungen zu rechnen. Aktuell werden beispielsweise Risiken durch „Air Gap Hacking" in Betracht gezogen: IP-Kameras könnten über einen angeschlossenen IR-Scheinwerfer mittels einer Art „Morsezeichen" vertrauliche Informationen nach außen senden, ohne dass dazu eine Netzwerkverbindung nötig ist.
Errichter sollten sich deshalb über neue Entwicklungen stets auf dem Laufenden halten, etwa bei „heise Security" [3].

Quellen & weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die erste Adresse für IT-Sicherheit in Deutschland. Es stellt kostenlos Dokumente mit Empfehlungen u.a. zum Sicherheitsmanagement und IT-Grundschutz zum Download bereit. Aktuell sind dort neue Bausteine zu embedded Systemen (IoT) und IP-Kameras erschienen.

Der BHE bietet umfangreiche Informationen zum Planen, Errichten und Betreiben von Videoanlagen, beispielsweise den „Praxisratgeber Videosicherheit" oder vielfältige Informationspapiere. Wissenswertes zum Thema Video lernen Errichter, Planer und Betreiber in den verschiedenen BHE-Seminaren.

[1] www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/IT-Grundschutz-Modernisierung/itgrundschutz_modernisierung_node.html

[2] www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_128.html

[3] www.heise.de/security/news

[4] www.heise.de/newsticker/meldung/Bericht-Ueberwachungskameras-mit-NSA-Hintertuer-weiter-vielerorts-im-Einsatz-3569958.html

[5] https://de.wikipedia.org/wiki/Virtual_Local_Area_Network

[6] www.bhe.de/de/Videoueberwachungstechnik

[7] www.bhe.de/file/software.pdf (BHE-Papier Software in Videosystemen)

[8] www.bhe.de/direkt/video/updates_vss.pdf

BHE e.V. | **Feldstr. 28, 66904 Brücken** | **Telefon: 06386 9214-0, Telefax: 06386 9214-99** | **Internet: www.bhe.de, E-Mail: info@bhe.de**