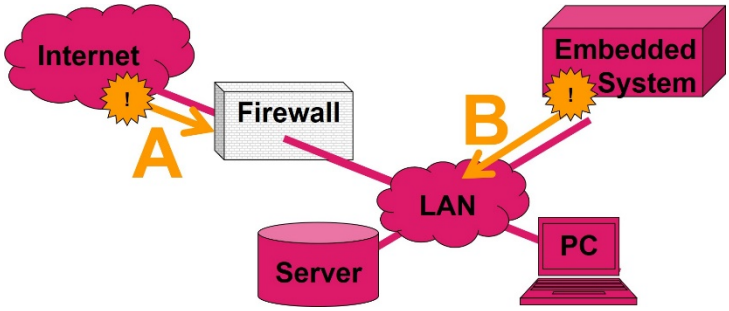
# 13. Cyber-Security bei Videosicherheitssystemen

## 13.1 Allgemeines

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.




## 13.2 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 bergen 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.

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.

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
- uvm.

## 13.3 Herausforderung IP

Für klassische Videosicherheitsanlagen hatte sich in der Vergangenheit 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

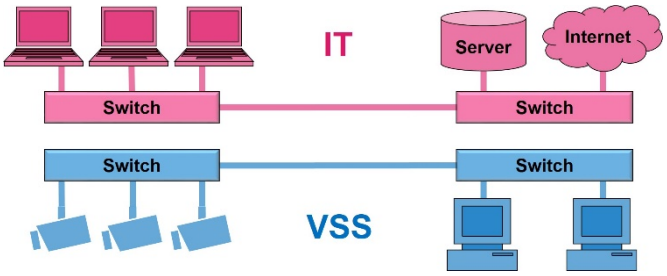
- Bequemlichkeit
- mangelnde Kenntnisse
- Kosten sparen „um jeden Preis“

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.

## 13.4 Lösungsalternativen

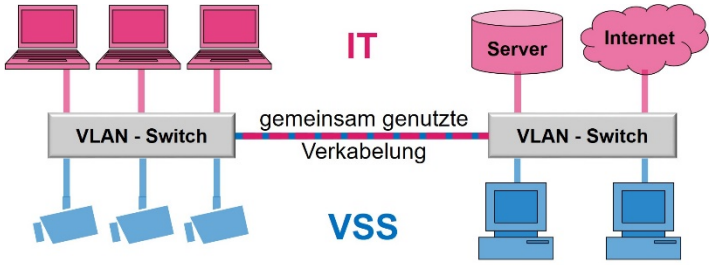
### 13.4.1 Einfach und sicher – separate Netze

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.



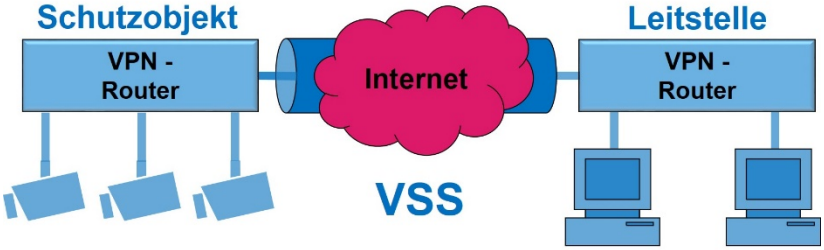

### 13.4.2 Mehrere Netze auf einem Kabel - VLAN

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.



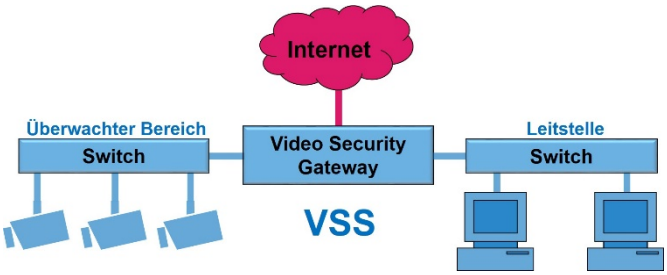

### 13.4.3 Ein sicherer Tunnel für Daten auf ihrem Weg durch das Internet – VPN

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.



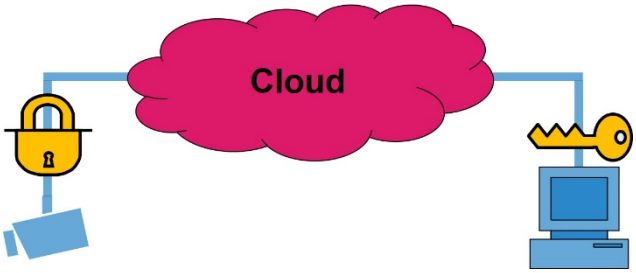

### 13.4.4 Sichere Verbindung nach außen – Video Security Gateway

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.




### 13.4.5 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?



## 13.5 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

## 13.6 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.

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.

Firewall Konfiguration am Beispiel Cisco ASDM