Cyber Security bei Videoanlagen

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

Von Hardo Naumann, Accellence Technologies

Intuitiv rechnen die meisten Menschen, wenn sie sich über Sicherheit Gedanken machen, mit Angriffen von außen. So ist es folgerichtig, dass bei den üblichen Firewall-Einstellungen vor allem Verbindungen, die von außen (aus dem Internet) nach innen (in das private Netz) aufgebaut werden, strengen Regeln unterliegen. Der Aufbau von Verbindungen von innen nach außen wird dagegen meist nicht oder nur wenig reglementiert, um den Zugriff der Anwender auf die verschiedenen weltweiten Internet-Anwendungen und Dienste nicht zu beeinträchtigen.

Unterschätztes Risiko „embedded Systeme“

PCs und Server werden als sicherheitsrelevante Technik bewusst wahrgenommen und (hoffentlich) entsprechend sorgfältig im Sicherheitskonzept berücksichtigt. Risiken, die von embedded Systemen wie etwa Produkten aus dem Smart-Home-Bereich, „intelligenten“ Lautsprechern, Alarmanlagen und auch Kameras ausgehen, werden dagegen häufig unterschätzt, weil bei diesen Geräten die Hauptfunktion im Blickpunkt steht. Eine IP-Kamera ist aber eben nicht nur eine Kamera, sondern ein kompletter vernetzter Computer mit allen Möglichkeiten und Risiken, die diese komplexe Technik bietet. Bei Entwicklung und Auswahl von embedded Systemen stehen meist Funktion und Preis im Vordergrund. Das hat zur Folge, dass die Datensicherheit oft vernachlässigt wird.

Embedded Systeme bringen ein Risiko mit sich, weil sie Verbindungen von innen nach außen durch die Firewall aufbauen können. Ist so eine Verbindung erst einmal hergestellt, können Angreifer darüber das Gerät steuern und das private Netz damit von innen angreifen.

Viele embedded Systeme 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.

Dass diese Risiken nicht abstrakt und theoretisch sind, sondern in der Praxis bereits zu erheblichem wirtschaftlichen Schaden geführt haben, zeigt eine Vielzahl von Beispielen:

- 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.

Spezialfall „Video Sicherheits Systeme“ (VSS)

Für klassische Videoüberwachungsanlagen hat sich die Abkürzung „CCTV“ etabliert. Das CC darin 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 nur genau die explizit gewünschten Verbindungen zulassen; dann können embedded Systeme keine Verbindung zu einem Angreifer aufbauen.

Lösungsalternativen

Das Risiko unerwünschter Verbindungen lässt sich durch geeignete technische Vorkehrungen vermeiden. Das ist vielleicht etwas aufwändiger und teurer, aber wenn die Sicherheit vernachlässigt wird, kann es auf lange Sicht sehr viel teurer werden.

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. Folgende Alternativen stehen zur Verfügung und können sich gegenseitig ergänzen:

1. Separates Netz für Video
Ein eigenes Netz für das VSS bietet die größte Sicherheit: Die physikalische Trennung von Leitungen kann von keiner Software überwunden werden. Höhere Kosten oder fehlende Kabeltrassen zwingen aber oft dazu, Video über vorhandene Leitungen zu transportieren. In diesen Fällen hilft

2. Virtual Local Area Network - VLAN
Mit einem VLAN kann die vorhandene Verkabelung genutzt werden, um mehrere logisch getrennte Netze zu realisieren. Dies erfordert durchgängig VLAN-fähige aktive Netzwerkkomponenten und eine konsequente fachgerechte Konfiguration.

3. Virtual Private Network - VPN
VPN ist das Mittel der Wahl wenn vertrauliche Daten über das Internet übertragen werden sollen. Alle Videodaten sind stets im LAN, VLAN und VPN zu halten, alle Verbindungen von und nach außerhalb dieses geschützten Bereichs sind zu sperren.

Wichtig dabei: Netzwerkkopplung vermeiden! Geräte, die an mehrere Netze angeschlossen sind, können ungewollt Verbindungen zwischen diesen Netzen herstellen. Alle Geräte dürfen deshalb nur an ein Netz angeschlossen werden. Sind weitere Kommunikationsbeziehungen nötig, so sollten diese nur realisiert werden über ein

4. Video Security Gateway
Ein „Video Security Gateway“ überwacht alle ein- und ausgehenden Verbindungen und kombiniert dabei verschiedene Sicherheitsmaßnahmen, die speziell auf die Belange der Videosicherheitstechnik im jeweiligen Anwendungsfall abgestimmt werden:

Die **Firewall** lässt nur die explizit gewünschten Verbindungen zu. Der **Router** stellt nach vorgegebenen Regeln Verbindungen her. Mittels Network Address Translation (**NAT**) werden dabei die IP-Adressen des internen Netzes vor der Außenwelt verborgen. Eine **DMZ** kann bei Bedarf eine Pufferzone zwischen äußerem und innerem Netz bilden. Die **Protokollanalyse** erkennt verdächtigen Datenverkehr. Ein **Virenscanner** prüft alle eintreffenden Daten auf Schadcode.

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 und wird nur spontan aktiv. Deshalb muss das Security Gateway dauerhaft alle Verbindungen überwachen, nicht nur die vom VSS genutzten.

5. Verschlüsselung
Eine durchgängige „Ende-zu-Ende-Verschlüsselung“ stellt sicher, dass niemand unbefugt auf die Videodaten zugreifen kann. Die Verschlüsselung kann alternativ auch im Video Security Gateway erfolgen. Dies ist insbesondere dann geboten, wenn Videodaten z.B. in der „Cloud“ gespeichert werden sollen. Entscheidend ist dabei: Wer besitzt den Schlüssel?

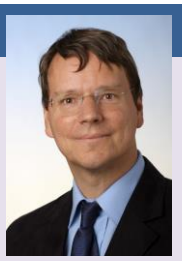
Weiterführende Informationen

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.

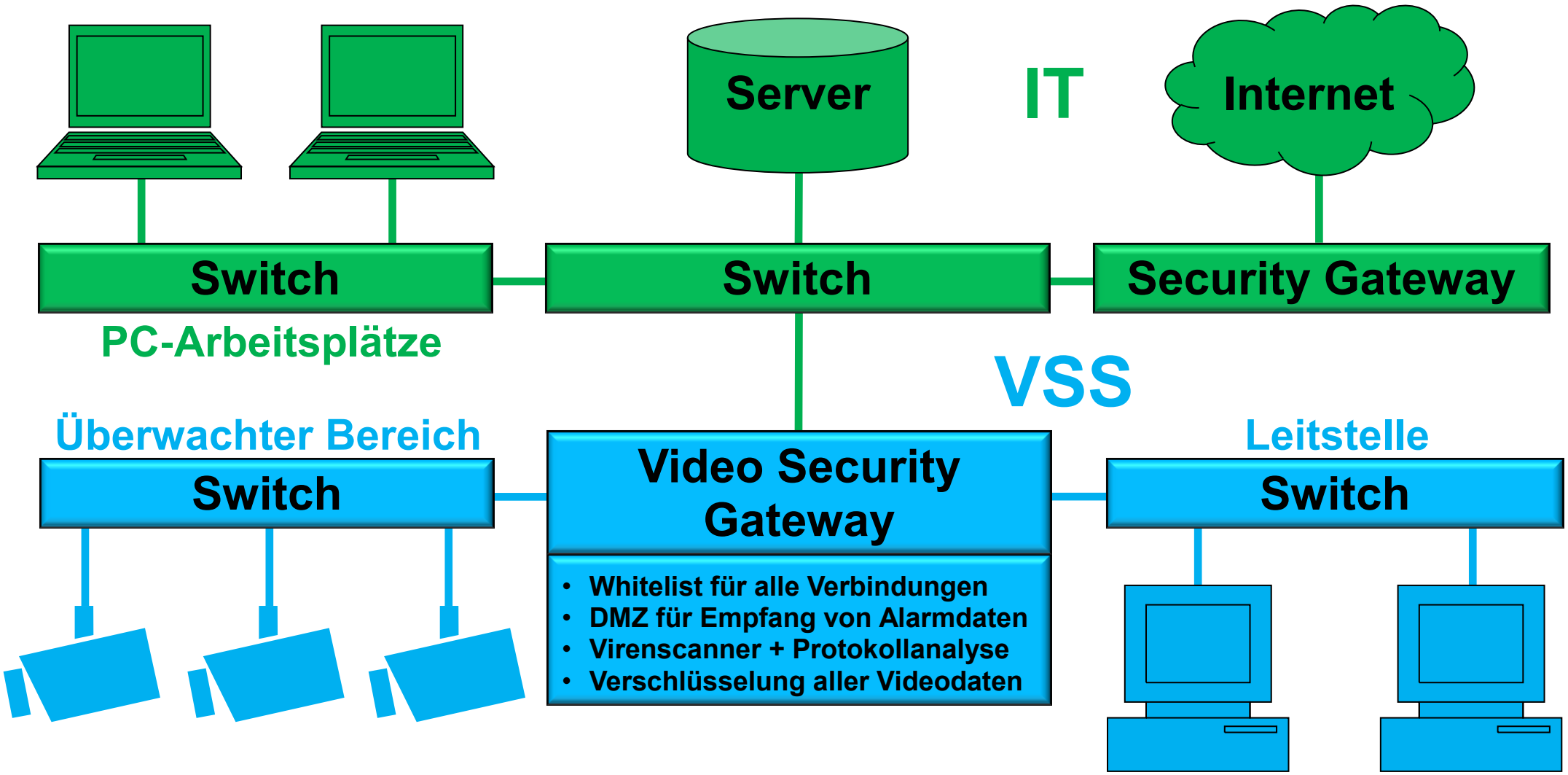
Im BHE Bundesverband Sicherheitstechnik e.V. arbeiten Hersteller und Errichter von Sicherheitssystemen zusammen. Der BHE veranstaltet Seminare und Kongresse, in Fachausschüssen werden Informationspapiere erarbeitet.

Holen Sie sich fachkundigen Rat, wenn Sie eine Videoanlage planen oder betreiben. Firmen wie Accellence Technologies in Hannover bieten umfassende Beratung und entwickeln spezielle Lösungen für die Videosicherheit.

Der Autor



Dipl.-Ing. Hardo Naumann ist General Manager für Alarm Receiving Solutions bei der Accellence Technologies GmbH und Mitglied im Fachausschuss „Video“ des BHE.



Kaskadierte Sicherheit: Ein Video Security Gateway sichert die Videoanlage gegenüber dem Unternehmensnetzwerk ab