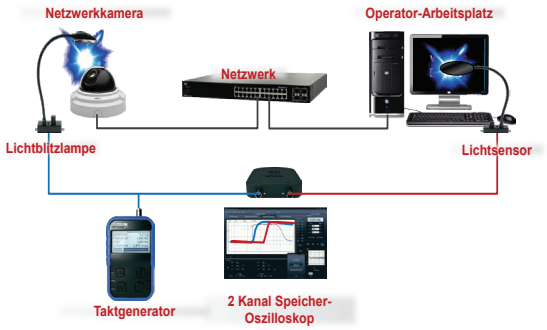
# Video-Überwachungstechnik

## *Sicherheit in IP-Netzen*

Die Sicherheit in IP-Netzen nimmt einen immer größer werdenden Stellenwert ein. Gerade in der Video-Überwachungstechnik, wo in der Regel personenbezogene Daten über IP-Netze übertragen werden, wird häufiger über „gesicherte Übertragungen“ (wie z.B. HTTPS = bekannt als sicheres Übertragungsprotokoll z.B. beim Übermitteln von banksensiblen Daten bei der Onlinebezahlung) diskutiert. Dieses Papier beschäftigt sich mit der Frage, inwieweit HTTPS für die Videoübertragung geeignet ist und welche Aspekte dabei zu berücksichtigen sind. Der Einstieg in dieses Thema ist nicht trivial, da es von Kameraherstellern kaum Leistungsdaten im HTTPS-Betrieb gibt.
Darüber hinaus wird die Frage, inwieweit Übertragungsleistungen (Anzahl der Bilder pro Sekunde) für VGA/HD/Full HD Kameras bei der HTTPS Übertragung zurückgehen, beantwortet.

Grundsätzlich ist das HTTPS-Protokoll für die Übertragung von Videosignalen aus Videoüberwachungsanlagen geeignet. Zunächst wurde die Übertragungsleistung bei verschiedenen Einstellungen mit folgendem Messaufbau gemessen:

Eine Blitzlampe erzeugt Lichtblitze im Takt eines Taktgenerators. Die Lichtblitze werden von einer handelsüblichen IP-Kamera aufgenommen und am Ende der kompletten Übertragungsstrecke auf einem Monitor angezeigt und von einem Lichtsensor registriert. Auf einem Speicher-Oszilloskop kann nun die Latenz als Zeitunterschied zwischen den Impulsen des Taktgenerators und den Signalen des Lichtsensors exakt abgelesen werden.




Die Bildrate (fps) wird mit Hilfe eines Screen-Recorders auf dem Operator-Arbeitsplatz gemessen. Die Messung wurde mit verschiedenen Browser-Typen und einem Videomanagementsystem VMS (Herstellername auf Anfrage möglich) jeweils bei den Videoauflösungen VGA (800x600 Pixel) und HD (1280x720 Pixel) durchgeführt:

| Videoanzeige erfolgte mit | **Latenz** [Millisekunden] HTTP → HTTPS | | **Bildrate** [fps] HTTP → HTTPS | |
|---|---|---|---|---|
| | **VGA** | **HD** | **VGA** | **HD** |
| Internet Explorer | 200 → 200 | 260 → 450 | 25 → 25 | 25 → 25 |
| Firefox | 200 → 200 | 220 → 350 | 25 → 25 | 25 → 25 |
| Chrome | 200 → 200 | 220 → 350 | 25 → 25 | 25 → 25 |
| Opera | 200 → 200 | 220 → 400 | 25 → 25 | 25 → 25 |
| VMS | 200 → 200 | 200 → 280 | 25 → 25 | 25 → 25 |

Ergebnisse für den Abruf von einem VGA oder HD-Videostream:

- Beim Umschalten von HTTP auf HTTPS hat sich die Bildrate nicht geändert.
- Die Latenz hängt nicht nur von der Kamera und dem gewählten Übertragungsprotokoll ab, sondern vor allem von der Effizienz der Wiedergabesoftware.

Ein anderes Bild zeigt sich, wenn die Kamera an ihre Leistungsgrenze gebracht wird:

- Bei gleichzeitigem Abruf per HTTP und HTTPS reduzierte sich die Bildrate bei HTTPS je nach verwendeter Anzeigesoftware unterschiedlich stark, bei HTTP blieb die Bildrate konstant bei 25 fps.
- Bei Erhöhung der Datenrate wurde die Latenz im Browser größer, beim Videomanagementsystem blieb sie nahezu gleich; die Bildrate sank ab ca. 25 Mbps bei HTTPS auf 12 fps.

Wie stark der HTTPS-Betrieb („HTTP Secure“ [1], Kombination von HTTP mit SSL/TLS [2]) die Übertragungsleistung für VGA/HD/Full HD Kameras reduziert, wird also maßgeblich bestimmt von der Leistungsfähigkeit der Kamera, der Parametrierung der Videoübertragung und der Effizienz der zur Wiedergabe verwendeten Software.

Ein signifikanter Unterschied der Videodatenraten zwischen HTTP- und HTTPS-Betrieb war bei den Messungen nicht festzustellen. Im Idealfall, also bei genügend Leistungsreserven in Kamera und Empfangsrechner sowie bei Verwendung besonders effizienter Software, hat der HTTPS-Betrieb keinen negativen Einfluss auf die Übertragungsleistung.

Die Messungen zeigen bei Nutzung des Browser-Plugins des Herstellers und expliziter Umschaltung auf H.264 identische Messwerte für HTTP und HTTPS. Unter dieser Randbedingung hat der Wechsel von HTTP auf HTTPS also auch keinen negativen Einfluss auf die Latenz. Daraus leitet sich ab, dass in der Praxis der Wechsel zum HTTPS-Betrieb einhergehen sollte mit der Wahl einer effizienten Kodierung wie z.B. H.264.

Mit dem Wechsel zum HTTPS-Betrieb soll das Ausspähen der Videodaten verhindert werden. Es muss dabei unbedingt darauf geachtet werden, dass die Videodaten auch tatsächlich über das HTTPS-Protokoll geführt werden. Wird die HTTPS-Verbindung alleine für die Konfiguration und die Steuerung der Kamera verwendet und wird parallel RTP als Protokoll für den Versand der Videodaten verwendet, dann bleiben die Videodaten unverschlüsselt.

Bei vielen Anlagen gibt es gute Gründe, das RTP-Protokoll für den Videodatenversand zu nutzen, z.B. wenn der Netzwerkverteildienstes „Multicast“ verwendet werden soll. Dieser Netzwerkverteildienst kann nur mit einem verbindunglosen Protokoll wie (RTP Real-time-Transport-Protocol [6]) genutzt werden. Damit auch bei dieser Konstellation die Videodaten abhörsicher übertragen werden, müsste das Protokoll SRTP (Secure Real-time-Transport-Protocol [3]) verwendet werden, wobei SRTP in der Praxis noch keine Rolle spielt mangels Produkten, die dieses Protokoll unterstützen.

Darüber hinaus muss man sich beim Wechsel zum HTTPS-Betrieb darüber im Klaren sein, dass die Videodaten nur während des Transportes abhörsicher sind. Sobald sie von der Videoempfangssoftware entgegengenommen werden, sind sie wieder unverschlüsselt. Wenn die Software die Videodaten dann unverschlüsselt abspeichert, könnten die Videodaten ggf. auf dem Speichermedium ausgespäht werden.

Wenn auch diese Lücke geschlossen werden soll, dann helfen nur Videomanagementlösungen, die eine durchgängige Ende-zu-Ende-Verschlüsselung beherrschen.

## Wird HTTPS von vielen Kunden als wichtig erachtet und aktiv nachgefragt?

HTTPS wird nicht häufig angefragt, aber die Tendenz ist steigend. Vielen Kunden bietet die klassische Authentifizierung (Digest access authentication) über HTTP für diesen Zweck ausreichenden Schutz [4].
HTTPS ergänzt HTTP um eine Verschlüsselung der übertragenen Daten mittels SSL/TLS. Ein Ausspäher könnte sonst sehen, was in der Kamera konfiguriert wird oder welche Schwenk/Neige/Zoom-Kommandos die Kamera erhält. Diese Inhalte sind aber oft nicht sicherheitsrelevant, so dass eine Verschlüsselung nicht unbedingt notwendig ist. Viel wichtiger ist die Verschlüsselung der eigentlichen Videodaten. Dafür kommen SRTP oder TLS in Frage.

## Wie viel „weniger“ an Sicherheit wird geboten, wenn nur die Passwörter verschlüsselt werden?

Verschlüsselte Passwörter können das Ausspähen von Videodaten nicht verhindern, wenn die eigentlichen Videodaten weiterhin unverschlüsselt übertragen werden. Das ist wie eine Schranke, die man auf freiem Feld aufstellt: Eindringlinge können daran einfach vorbeifahren.
Mit einem Netzwerksniffer (z.B. WireShark oder Packetizer) können Hacker die auf dem Netz übertragenen Videodaten mitschneiden und sichtbar machen. Ebenso kann die Konfiguration (welche im Klartext via HTTP erfolgt) mitgeschnitten werden).
In einem geswitchten LAN, wie sie heute weit verbreitet sind, ist dies etwas schwieriger, aber nicht unmöglich.

## Verschlüsseln alle Hersteller auch die Videodaten (Stream, RTSP) oder nur die Übermittlung von Parametern?

Die Verschlüsselung der Videodaten wird nicht von allen Herstellern unterstützt, daher ist dies im Einzelfall zu prüfen. Wenn Kamera- bzw. Rekorder-Hersteller keine Verschlüsselung der Videodaten unterstützen, dann sollte das Videomanagementsystem die Daten zum frühestmöglichen Zeitpunkt verschlüsseln. Bei sensiblen Kameras sollte das Videomanagementsystem einen speziellen Verschlüsselungsadapter vorschalten, so dass die Kamera nicht direkt mit dem Netzwerk verbunden ist.

## Ergeben sich in großen Netzwerken Probleme mit HTTPS?

Grundsätzlich nein, wenn einige Punkte beachtet werden: Je nach Netzwerk müssen die Firewalls entsprechend konfiguriert sein. Bei größeren Installationen sollte man prüfen, inwieweit es Performance-Einschränkungen auf der Seite der Video-Management-Software (VMS) gibt, denn sie muss bei einer größeren Anzahl von Kanälen alle Videoströme entschlüsseln.

Zudem unterstützen nicht alle VMS-Lösungen HTTPS. Wichtig ist auch zu beachten, dass bei TCP-basierten Protokollen wie HTTPS nicht der Datenverteildienst Multicast oder Broadcast eines IP-Netzwerkes genutzt werden kann. Das wirkt sich besonders dann aus, wenn eine Videoquelle auf viele Videoanzeigen aufgeschaltet werden soll. Bei HTTPS muss die Videoquelle die Streams für jeden Abnehmer selbst zur Verfügung stellen. So viele Verbindungen können die Quelle (Netzwerkkamera) überlasten. Bei SRTP in Verbindung mit Multicast wird die Quelle dagegen nur einmal belastet; das Netzwerk verteilt bei Multicast die Daten an alle Videoanzeigen.

## Weitere Aspekte

Bei der Auslegung von Videosicherheitsanlagen ist die Europa-Norm EN 50132-7 zu beachten. Wo möglich und soweit wirtschaftlich vertretbar, sollte für Video ein separates Netzwerk vorgesehen werden. Bei größeren Installationen, bei denen via Remote-Anbindung auf mehrere Kameras zugegriffen werden soll, erfolgt die Anbindung meistens über einen VPN-Tunnel, der zwischen den Gateways aufgebaut wird. Mittels solcher Konfigurationen wird die Aufgabe der Verschlüsselung auf die Gateways verlagert. Auch IEEE 802.1X sollte in diesem Zusammenhang in Betracht gezogen werden [5].

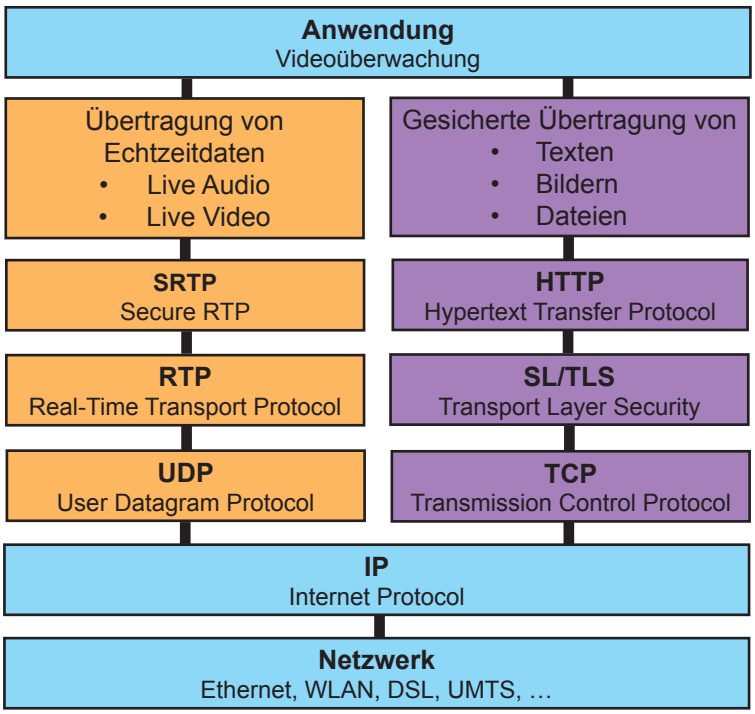
Auch die Leistungsdaten des vorhandenen Netzwerks sowie der Verbindung ins Internet (Upload) sind zu beachten. Vor allem hängt es von der Anzahl der Kameras, deren Auflösung und der Komprimierung der Daten ab, ob Bilder flüssig wiedergegeben werden können. Eine Wiedergabe der Videos in Videomanagementsystemen ist häufig effizienter als eine Anzeige im Browser.

Wenn man Bedenken wegen des Ausspähens der Videodaten im eigenen Betrieb ausräumen will, darf nicht nur das Netzwerk als Angriffspunkt gesehen werden. Um den Anforderungen von Datenschützern und Betriebsrat gerecht zu werden, muss das gesamte System betrachtet werden. Denn beispielsweise kann auch die Dateiablage der Videos eine potenzielle Sicherheitslücke sein.
Um das Gesamtsystem zuverlässig abzusichern muss eine Ende-zu-Ende Verschlüsselung verwendet werden, bei der die Videodaten nicht nur verschlüsselt übertragen, sondern auch verschlüsselt

aufgezeichnet werden. In diesem Falle erfolgt die Verschlüsselung mit einem öffentlichen Schlüssel direkt auf der Kamera und die Entschlüsselung mit einem privaten Schlüssel, der sich z.B. auf einem Dongle als „Security Token“ befindet [7]. Übertragung, Speicherung und Weiterleitung der Daten erfolgen dabei ausschließlich in verschlüsselter Form. Die hocheffizienten Algorithmen erzeugen nur eine minimale Latenz und ermöglichen damit auch eine quasi verzögerungsfreie PTZ-Steuerung der Kamera.
Um auch die Sicherheitslücke durch die Systemadministration zu schließen, ist schließlich auch ein solides Schlüsselmanagement erforderlich, weil die Schlüssel für die Videodatenübertragung ausschließlich durch dedizierte Personen bzw. Instanzen in das System eingebracht werden können, z.B. über eine PublicKey-Infrastructure.

## Überblick Protokollstruktur

Das nebenstehende Diagramm zeigt, wie die verschiedenen Protokolle für den Anwendungsfall „Videoüberwachung“ aufeinander aufbauen.




TCP stellt durch im Protokoll eingebaute Rückmeldungen sicher, dass verlorengegangene oder fehlerhafte Daten erneut angefordert werden. Dies ist für die Übertragung von Texten, Bildern oder Dateien sehr sinnvoll. Bei Übertragung von Echtzeitdaten wie Live-Audio oder -Video kann es bei mangelnder Kanalkapazität jedoch zu einem Datenstau beim Sender führen. Eine IP-Videokamera muss deshalb eine Strategie implementieren, Audio-/Video-Echtzeitdaten im Falles eines Datenstatus zu verwerfen. Gute Implementierungen regeln die Bildrate in Abhängigkeit der verfügbaren Kanalkapazität.

Datenverluste kann der Sender bei RTP nicht von sich aus feststellen, er wäre auf Rückmeldungen des Empfängers angewiesen. Das ist über RTCP (RealTime-Control-Protocol) zwar vorgesehen, wird aber in der Praxis von den Kameraherstellern kaum ausgewertet. Das führt dazu, dass in der Praxis bei verlustbehafteten Übertragungsstrecken mit HTTP/TCP oft eine bessere Übertragungsleistung erzielt wird als mit RTP/UDP.

**Quellenangaben / Weiterführende Informationen**


[1] http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure
[2] http://de.wikipedia.org/wiki/Transport_Layer_Security
[3] http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol
[4] http://de.wikipedia.org/wiki/HTTP-Authentifizierung
[5] http://de.wikipedia.org/wiki/IEEE_802.1X
[6] https://de.wikipedia.org/wiki/Real-Time_Transport_Protocol
[7] http://www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/1124038
[8] http://www.funkschau.de/datacenter/artikel/120832
[9] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf


*Bei tiefergehenden Fragen kann auf Wunsch ein Expertenkreis aus dem BHE-Fachausschuss Videoüberwachungstechnik (FA-VÜT) konsultiert werden (Kontakt über BHE-Geschäftsstelle).*




**BHE - Feldstraße 28**
**66904 Brücken**
**Telefon: 06386 9214-0**
**Telefax: 06386 9214-99**
**Internet: www.bhe.de**
**E-Mail: info@bhe.de**