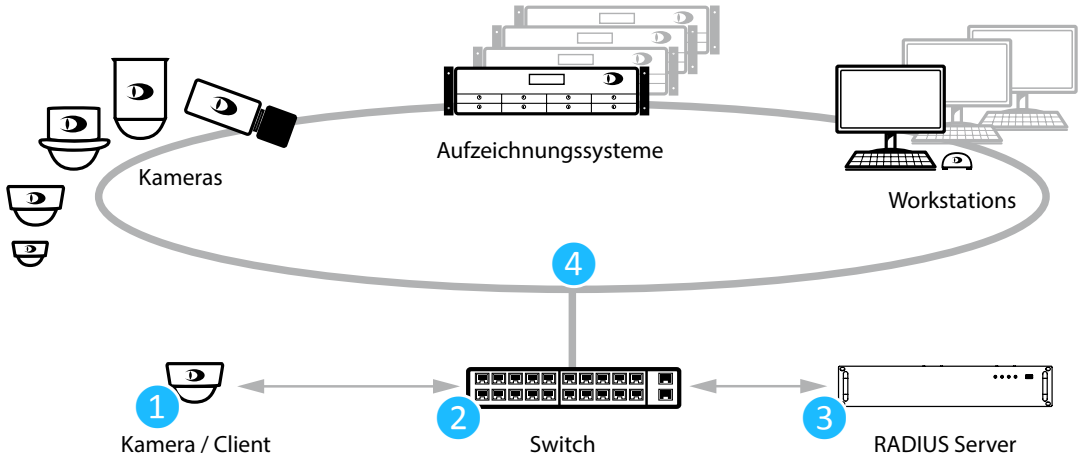
Sichere Netzwerkauthentifizierung

Absicherung des Video-Netzwerks durch Netzwerkauthentifizierung gemäß IEEE 802.1X

Die **Kameras der Serie 5000** wurden mit einem besonderen Augenmerk auf die **Systemsicherheit** entwickelt und unterstützen die **sichere Netzwerkauthentifizierung** (IEEE 802.1X) sowie die **verschlüsselte Daten- und Video-Übertragung** (TLS/AES-256). Weitere Sicherheitsmaßnahmen umfassen die Benutzerverwaltung, den Passwortschutz, die Deaktivierung nicht benötigter oder unsicherer Ports, die regelmäßige Bereitstellung von Firmware-Updates sowie die Verhinderung der Ausführung von Fremd-Software.

Betreiber von Videoanlagen zur Absicherung von öffentlichen Plätzen, Flughäfen, Casinos oder Unternehmen sind in der Regel mit dem Problem konfrontiert, dass **Kameras am physischen Rand des Netzwerks montiert** sind. Da diese Kameras für Dritte zugänglich sind, erhöht sich das **Risiko eines ungewollten Zugriffs auf das Netzwerk**. Ein Angreifer könnte statt der Kamera ein eigenes Gerät anschließen, um Zugang zum Netzwerk zu erhalten oder den Datenverkehr auszulesen (Man-in-the-Middle-Angriff).

Neben einer manipulationssicheren Montage der Kameras kann dieses Risiko vor allem durch den **Aufbau eines Netzwerks mit einer Authentifizierung nach dem Standard IEEE 802.1X** abgeschwächt werden. Dabei bietet sich der **Einsatz der Kamera-Serie 5000** an, denn alle Modelle unterstützen die Authentifizierung anhand von Zertifikaten (EAP-TLS) gemäß IEEE 802.1X.



1 Kamera

Die Kamera wird mit einem individuellen Zertifikat (Ausweis) ausgestattet, bevor sie an das Netzwerk angeschlossen wird.

Wenn die Kamera mit dem Netzwerk verbunden wird, baut sie eine Verbindung über einen Netzwerk-Port (Tür) auf. Diese Verbindung ist beschränkt (Türklappe) und erlaubt nur die Sendung einer Anfrage mit dem Zertifikat an einen Access-Switch (Türsteher).

Ein beliebiger Client (Angreifer) könnte hier irgendein Zertifikat übergeben. Der Zugriff auf das Netzwerk wäre aber auf die Kommunikation mit dem Switch beschränkt.

2 Switch

Der Switch prüft die grundlegende Zulässigkeit der Anfrage (Passfoto) und leitet das Zertifikat an den RADIUS Server (Club-Besitzer) weiter.

Ein Angreifer mit einem schlecht gefälschten Zertifikat würde bereits hier abgewiesen werden. Der entsprechende Port könnte automatisch komplett gesperrt werden.

3 RADIUS Server

Der RADIUS Server führt eine gründlich Prüfung des Zertifikats durch. Dies kann durch einen Vergleich mit hinterlegten Zertifikaten erfolgen (Kundenkartei), aber auch durch einen Abgleich der Daten mit einem LDAP-Server (Meldebehörde).

Alle Zertifikate sind mehrstufig mit HASH-Codes signiert. Eine erfolgreiche Fälschung durch einen Angreifer kann ausgeschlossen werden.

4 Zugriff

Wenn der RADIUS Server die Gültigkeit des Zertifikats und die Berechtigung des Inhabers (Kamera) zum Netzwerkzugriff feststellt, sendet er eine entsprechende Bestätigung (Einlass) an den Switch.

Ein Angreifer mit einem gültigen Zertifikat, aber ohne Berechtigung zum Netzwerkzugriff, würde hier endgültig abgewiesen werden.

Der Switch öffnet in diesem Fall den Netzwerk-Port (Tür) vollständig, und die Kamera kann eine unbeschränkte Netzwerkverbindung (Eintritt) herstellen.

Wenn entsprechende Rollen definiert sind, kann der Switch den Netzwerkzugriff auf bestimmte VLAN-Teilbereiche (Tanzfläche, Bar) beschränken.

Nach der erfolgreichen Authentifizierung kann die Kamera einen normalen Netzwerkstart durchführen.

Allgemeines

- Wenn die Netzwerkverbindung einer Kamera getrennt wird, erkennt und meldet das Dallmeier Aufzeichnungssystem automatisch einen Ausfall.
- Bei fehlender Authentifizierung ist kein Netzwerkzugriff und kein Auslesen des Datenverkehrs möglich.
- Ports mit fehlgeschlagegen Authentifizierungsversuchen können automatisch gesperrt werden (keine Anfrage mehr möglich).

Dieses Handout beschreibt IEEE 802.1X stark vereinfacht. Detaillierte technische Informationen finden Sie unter https://de.wikipedia.org/wiki/IEEE_802.1X.