Mirko Dölle

Passwort-Petze

Passwortverrat und Firewall-Untertunnelung bei Foscam-Kameras – und wie man es unterbindet

Dank Plug and Play können Laien selbst komplexe Geräte ganz ohne Fachkenntnisse in Betrieb nehmen. Hersteller Foscam macht es Kunden bei seinen Netzwerkkameras besonders einfach. Sicherheit und Datenschutz bleiben dabei aber gefährlich auf der Strecke.

Die bequeme Einrichtung komplexer Geräte wie Netzwerkkameras ist für Kunden durchaus ein Kaufargument, weshalb Hersteller den Kunden die Inbetriebnahme so leicht wie möglich machen wollen. Foscam hat für die Konfiguration seiner Netzwerkkameras verschiedene Wege vorgesehen, etwa die Konfiguration im Browser oder per Barcode und App. Sicherheit und Datenschutz sind allerdings nicht immer gewährleistet.

Das mit Ethernet und WLAN ausgestattete Modell FI9900P bietet ein Web-Frontend für die Konfiguration. Die Nutzung ist scheinbar einfach: Hat man die Kamera per Kabel an den heimischen Router angeschlossen, sucht man die vom DHCP-Server vergebene IP-Adresse heraus und kontaktiert auf Port 88 den integrierten Webserver. Einloggen kann man sich allerdings erst, wenn man das proprietäre Windows-Programm IPC Web Components von der Kamera heruntergeladen und installiert hat – wovor Windows warnt, da es ja aus keiner vertrauenswürdigen Quelle stammt.

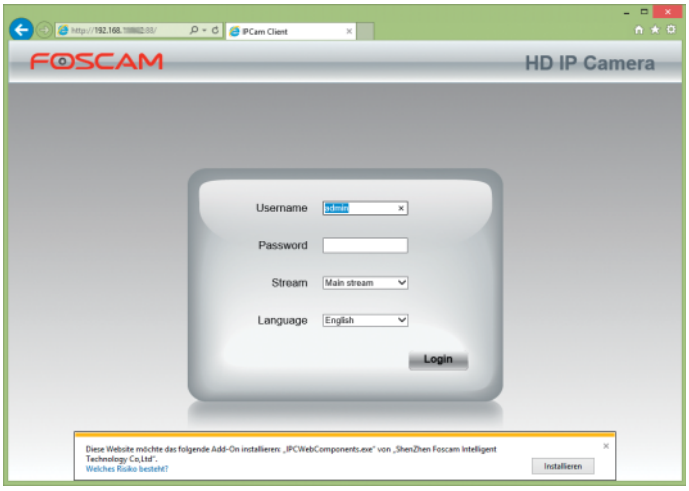
Zwangsregistrierung

Das Web-Frontend erlaubt nicht nur die Konfiguration von WLAN, Videoeinstellungen, Bewegungserkennung und Benutzerverwaltung der Kamera, Sie können sich auch das Livebild ansehen. Um auch von unterwegs zu Hause nach dem Rechten sehen zu können, gibt es die kostenlose Foscam-App für Android und iPhone. Die Gestaltung und Funktionalität der App ist auf beiden Systemen gleich, von Umlautproblemen unter iOS einmal abgesehen. Startet man die App, muss man sich zunächst mit einer E-Mail-Adresse bei Foscam registrieren, wobei die Adresse über eine Aktivierungs-Mail überprüft wird.

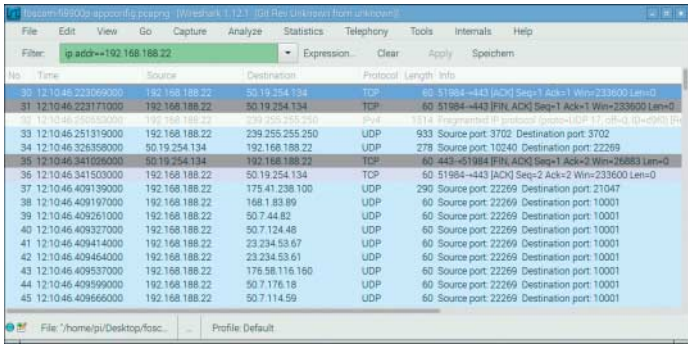
Eine per Web-Frontend konfigurierte Kamera fügen Sie hinzu, indem Sie das Mobilgerät mit dem WLAN verbinden, in dessen Subnetz sich auch die Kamera befindet, und dann die URL bestehend aus IP-Adresse und Port 88 der Kamera eingeben. Für den Zugriff auf die Kamera verlangt die App noch Benutzername und Passwort der Kamera – wobei es sich um einen Admin-Zugang handeln muss, mit weniger Rechten gibt sich die App an dieser Stelle nicht zufrieden. Dafür können Sie mit der App auch einige Teile der Konfiguration anpassen oder Firmware-Updates einspielen.

Passwort-Verräter

Haben Sie mehrere Mobilgeräte, können Sie auch dort die Foscam-App installieren. Ab dem zweiten Gerät genügt es, wenn Sie beim ersten Start Benutzername und Passwort aus der App-Registrierung bei Foscam eingeben – die Kameras auf dem zweiten Mobilgerät neu einzurichten



Das Web-Frontend hat Foscam mit einem proprietären Windows-Programm verdongelt, das man sich erst von der Kamera herunterladen und installieren muss.



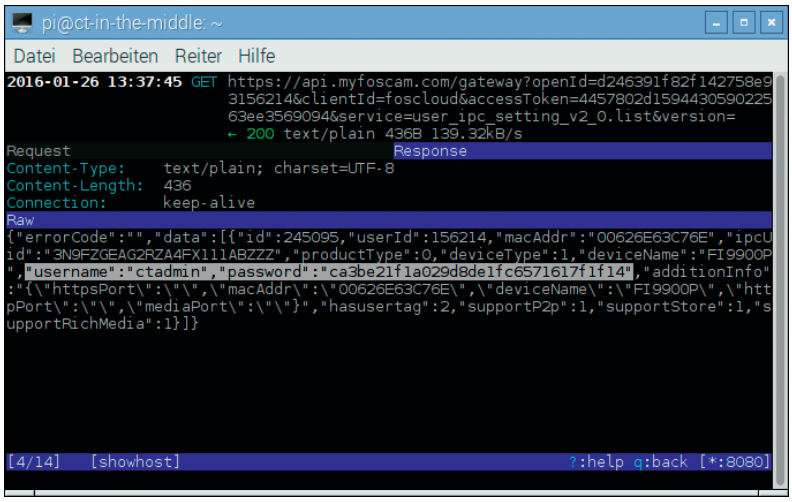
Kaum wurde die Kamera eingeschaltet, öffnet sie etliche Verbindungen zu verschiedenen Servern. Mindestens einer davon gehört laut Reverse-Lookup zu einem VPN-Dienstleister.

ist nicht erforderlich, sie sind bereits da. Sogar inklusive Benutzernamen und Admin-Passwort. Die Foscam-App speichert nämlich Admin-Benutzer nebst Passwort, Geräte-ID und MAC-Adresse auf dem Server des Herstellers – und ruft sie bei jedem Start dort wieder ab.

Für den Kunden ist das praktisch, kann er doch problemlos die Zugangsdaten einer Kamera verändern oder weitere Kameras hinzufügen, ohne die Konfiguration auf allen Mobilgeräten anpassen zu müssen. Allerdings benötigt man auch eine große Portion Vertrauen in die Fähigkeiten des Herstellers, den Server mit den Zugangsdaten gegen Hacker und Nachrichtendienste abschirmen zu können – denn mit Hilfe des Admin-Passworts kommt man auch jederzeit an die WLAN-Einstellungen und so an die SSID und den WLAN-Key des drahtlosen Netzwerks heran. Schlimmer noch, ein Angreifer könnte die erbeuteten Zugangsrechte nutzen, um der Kamera eine kompromittierte Firmware unterzuschieben und sich so einen Brückenkopf für weitere Angriffe zu schaffen.

Zweifel an den Fähigkeiten der Foscam-Entwickler sind durchaus angebracht: So störte es die iOS-App nicht im Geringsten, dass wir ihr bei unserem Man-in-the-Middle-Angriff gefälschte Zertifikate unterschoben. Mehr als einen Raspberry Pi mit WLAN-Adapter braucht es dafür nicht.

Potenziellen Angreifern hilft auch, dass die Kamera sofort nach dem Einschalten nach Hause telefoniert und Tunnel nutzt, um lokale Firewalls zu durchlöchern. So beobachteten wir nur wenige Sekunden nach Einschalten reproduzierbar, wie die Kamera bis zu zehn UDP- und (SSL-verschlüsselte) TCP-Verbindungen zu verschiedenen Servern im Internet aufbaute. Eine der Verbindungen führte in der Regel zu einem Server aus dem Subnetz 50.7.0.0/16, häufig zu 50.7.44.82. Ein Reverse-Lookup der Adresse ergab, dass es sich dabei um einen Server des VPN-Dienstleisters vpnbaron.com handelt. Die anderen Server stammten aus verschiedenen Netzen, den Rückwärtsauflösungen zufolge scheinen auch Server aus Amazons Web Service (AWS) zum Einsatz zu kommen. Welche Daten die Kamera mit den Servern austauscht und ob die Daten innerhalb eines VPN weitergeleitet werden oder nicht, konnten wir aufgrund der Verschlüsselung nicht feststellen.



Erwischt: Die Foscam-App bekommt von Foscams Server api.myfoscam.com sämtliche Daten der Kamera inklusive Admin-Zugang und Passwort mitgeteilt.

Firewall durchlöchert

Unser Versuch, die SSL-Verschlüsselung mit unserem Raspberry Pi und eigenen Zertifikaten auszuhebeln, scheiterte – wann immer wir der Kamera gefälschte Zertifikate präsentierten, kam keine SSL-Verbindung zustande. Hier haben die Entwickler offenbar gründlicher gearbeitet als bei der App. Daher können wir nicht mit Gewissheit sagen, welche Daten die Kamera überträgt. Wir fragten bei Foscam nach, eine Erklärung für den Zweck der SSL-Verbindung bekamen wir nicht. Durch die Beobachtung des Kommunikationsverhaltens konnten wir allerdings einige beunruhigende Schlüsse ziehen.

So vermittelt der Foscam-Server offenkundig zwischen App und Kamera einen UDP-Tunnel für die Videoübertragung. Dabei kommt die UDP-Punchhole-Technik zum Einsatz, wofür zunächst App und Kamera jeweils einen UDP-Tunnel zum Foscam-Server aufbauen und so die Firewall des DSL-Routers oder Firmennetzes durchlöchern. Damit die verschickten UDP-Pakete der Kamera beantwortet werden können, gibt die Firewall des Routers den verwendeten Port für eingehende Verbindungen frei und leitet die dort eingehenden Daten an die Kamera weiter.

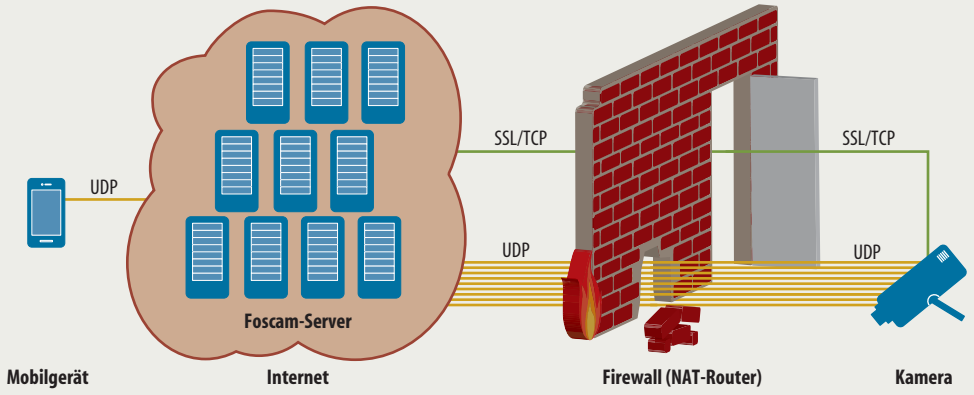
Das nutzt der Foscam-Server aus und übermittelt der App die öffentliche IP-Adresse und den von der Kamera verwendeten UDP-Port – woraufhin die App ihre Datenpakete an die genannte IP-Adresse und den Port sendet und so einen Tunnel zur Kamera aufbauen kann. Umgekehrt verwendet die Kamera die öffentliche IP-Adresse und den von der App benutzten Port, um ihre Daten anschließend direkt zu übertragen. Das hat den Vorteil, dass die App die Kamera auch aus einem fremden Netzwerk heraus erreichen kann – sie durchlöchert die Firewall des Routers, in dem sich das Mobilgerät mit der App befindet, aber gleichermaßen.

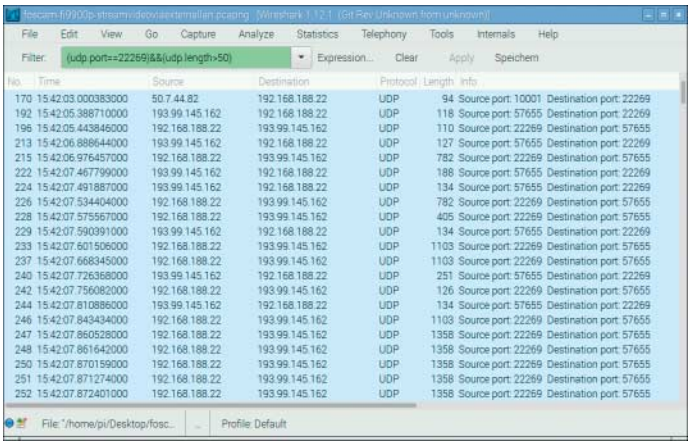
Das konnten wir mit Wireshark auf unserem Raspberry Pi leicht nachvollziehen, wie die Abbildung auf Seite 76 oben zeigt: Der zunächst für die Verbindung zum Foscam-Server 50.7.44.82 genutzte UDP-Port 22269 wird kurze Zeit später von der öffentlichen IP-Adresse unseres Internet-Anschlusses kontaktiert, anschließend werden größere Datenpakete übertragen – der Video-Stream.

Können App und Kamera die Firewall nicht durchstoßen, etwa

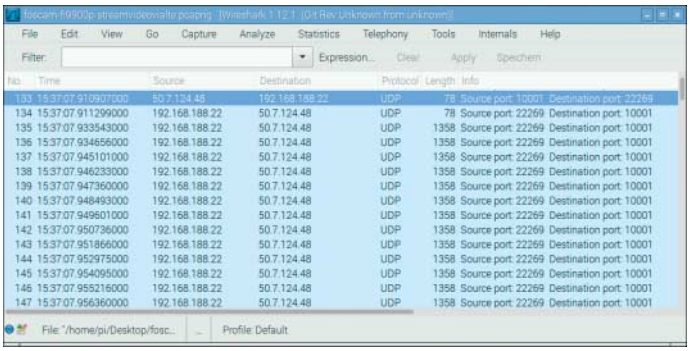
Unheimlich kontaktfreudig

Die Foscam-Kamera ist äußerst kontaktfreudig, schon kurz nach dem Einschalten nimmt sie Kontakt mit bis zu zehn Servern aus diversen Adressbereichen auf. Per UDP-Punchhole wird dabei die Firewall durchlöchert.





UDP-Tunnel per Punchhole: Die App übernimmt für die UDP-Verbindung den Port, der zuvor von der Kamera für die Kommunikation mit dem Foscam-Server genutzt wurde.



Können App und Kamera ihre Firewalls nicht für eine direkte Verbindung durchlöchern, sendet die Kamera Video-und Audio-Daten kurzerhand an den Hersteller – der das Material hoffentlich nur an die App weiterleitet.

aufgrund einer restriktiven Firewall-Konfiguration oder weil das Mobilgerät das Mobilfunknetz zur Datenübertragung verwendet, springt der Foscam-Server kurzerhand als Proxy ein. So landen sämtliche Video- und Audiodaten der Kamera direkt bei Foscam. Auch diese Funktion ließe sich von einem Angreifer mit Leichtigkeit von außen triggern, wenn er die Kontrolle über den Foscam-Server erlangt hat – der feuchte Traum eines jeden Nachrichtendienstes, bei dem das Opfer seine Überwachung sogar selbst erledigt und auch noch dafür bezahlt!

Her mit dem WLAN-Key

Der beschriebene lasche Umgang mit Passwörtern und persönlichen Daten gegenüber dem Hersteller lässt die höchst komfortable Ersteinrichtung der Foscam-Kameras mit Hilfe der App in einem anderen Licht erscheinen. Ist die Kamera noch nicht konfiguriert, schließen Sie sie per Ethernet an Ihren Router an und fotografieren den auf dem Typenschild aufgedruckten 2D-Barcode aus der App heraus. Der Barcode enthält die UUID des Geräts, über die sich die Kamera eindeutig identifizieren lässt. Sofort danach verlangt die App die Eingabe der WLAN-SSID und des WLAN-Schlüssels – trotz der bestehenden Ethernet-Verbindung und obwohl sie sich bereits bei Foscams Servern gemeldet hat. Dieser Schritt lässt sich auch nicht überspringen, ohne Eingabe des WLAN-Passworts lässt sich die Kamera nicht einrichten.

Währenddessen kommuniziert die App munter mit mehreren Servern – SSL-verschlüsselt. Welche Daten genau übertragen werden, lässt sich selbst nach Aushebeln der Verschlüsselung nicht sagen: Es handelt sich zum Teil um Binärdaten ohne sichtbare Struktur, die Datenmenge beträgt etliche hundert Bytes. Immerhin dürfen Sie beim WLAN-Key schummeln: So funktioniert die Einrichtung auch, wenn Sie in der App einen falschen WLAN-Schlüssel eingeben – die App überprüft ihn nicht und die Kamera übernimmt ihn bei bestehender Ethernet-Verbindung auch nicht.

Maulkorb

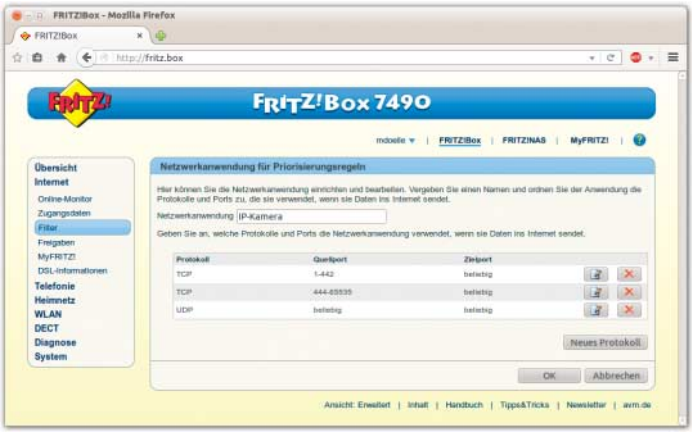
Aufgrund der Mitteilsamkeit und Kontaktfreudigkeit durch alle Firewalls hindurch ist der Betrieb der Foscam-Kamera in einem Firmennetz oder zu Hause unverantwortlich. Sie öffnet einem Angreifer, der Zugriff auf Foscams Server erlangt hat, ein Scheunentor zum Ausspähen und für Angriffe aller Art. Mit Kindersicherungen oder der Firewall von DSL-Routern wie der AVM Fritzbox können Sie der Kamera aber einen wirksamen Maulkorb verpassen – ohne auf den Zugriff aus der Ferne verzichten zu müssen.

Wichtigster Punkt ist, dass Sie vor dem ersten Einschalten der Kamera zunächst die DSL-Verbindung Ihres Routers unterbrechen – indem Sie einfach den Stecker ziehen. Haben Sie die Kamera angeschlossen und eingeschaltet, erfragt sie per DHCP eine IP-Adresse des Routers und macht sich so dem Router gegenüber bekannt. Nun können Sie die Kindersicherung verwenden, um der Kamera jeglichen Zugriff auf das Internet zu entziehen – und zwar sowohl für TCP als auch für UDP.

Damit kann die Original-App des Herstellers allerdings keine Verbindung mehr aufbauen – die Vermittlung erfolgt stets, auch im lokalen Netz bei Angabe der lokalen IP-Adresse, über den Server des Herstellers. Alternative IP-Kamera-Apps, die in großer Anzahl angeboten werden und häufig auch Foscam-Kameras unterstützen, haben dieses Problem nicht: Sie verwenden lediglich den Webserver, um auf die Kamera zuzugreifen und den Videodatenstrom abzurufen. Die sicherste Lösung ist, den Apps auf den Mobilgeräten über eine VPN-Verbindung zum DSL-Router Zugriff auf das heimische Netz zu verschaffen und die Kamera über ihre lokale IP-Adresse anzusprechen.

Alternativ können Sie im DSL-Router eine Port-Weiterleitung einrichten, vorzugsweise auf den SSL-Port 443 der Kamera, sodass der Datenverkehr sogar verschlüsselt abläuft. Damit die Kindersicherung das erlaubt, benötigen Sie ein angepasstes Profil und fügen eine neue Netzwerkanwendung hinzu. Die Abbildung unten zeigt die Konfiguration für die Fritzbox: Hier geben Sie für die Anwendung „IP-Kamera“ alle UDP-Verbindungen und alle TCP-Verbindungen mit Ausnahme von Port 443 an. Danach erstellen Sie ein neues Zugangsprofil „IP-Kamera“, bei dem Sie „IP-Kamera“ als gesperrte Anwendung eintragen – womit sämtliche Ports bis auf Port 443 TCP blockiert werden. Abschließend weisen Sie in der Kindersicherung Ihrer Kamera „IP-Kamera“ als Zugangsprofil zu und übernehmen die Änderungen.

Jetzt können Sie das DSL-Kabel wieder an Ihren Router anschließen und sicher sein, dass die Foscam-Kamera keine unerwünschten Verbindungen mehr aufbaut. (mid@ct.de)



Maulkorb für die Kamera: Sämtliche Ports mit Ausnahme des SSL-Webservers werden dem Kamera-Anwendungsprofil hinzugefügt und später mittels Kindersicherung blockiert. c't