

# Independent Tests of Anti-Virus Software



## **IP Kamera Test 2020** **Im Auftrag von PC Magazin**

TESTZEITRAUM: MAI 2020  
SPRACHE: DEUTSCH  
LETZTE REVISION: 3. JUNI 2020

[WWW.AV-COMPARATIVES.ORG](http://WWW.AV-COMPARATIVES.ORG)



# Inhalt

<b>EINLEITUNG</b>	<b>3</b>
<b>TESTUMGEBUNG</b>	<b>3</b>
<b>TESTMETHODE</b>	<b>4</b>
<b>PRODUKTE IM TEST</b>	<b>5</b>
<b>TESTERGEBNISSE</b>	<b>5</b>
<b>FAZIT</b>	<b>12</b>
<b>COPYRIGHT AND DISCLAIMER</b>	<b>13</b>

## Einleitung

Im Auftrag von PC Magazin sollen sechs Überwachungskamerasysteme für den Heimgebrauch auf ihre Sicherheitseigenschaften untersucht werden. Sowohl die Testgeräte, Testmethode als auch die Testkriterien, anhand welcher die Kamerasysteme bewertet werden sollen, sind vom Auftraggeber vorgegeben. Darüber hinaus haben wir nach unserem Ermessen die Testkriterien durch weitere sicherheitsrelevante Eigenschaften ergänzt. In den folgenden Abschnitten werden der Testaufbau und die angewandte Testmethode näher beschrieben sowie die getesteten Produkte aufgelistet.

## Testumgebung

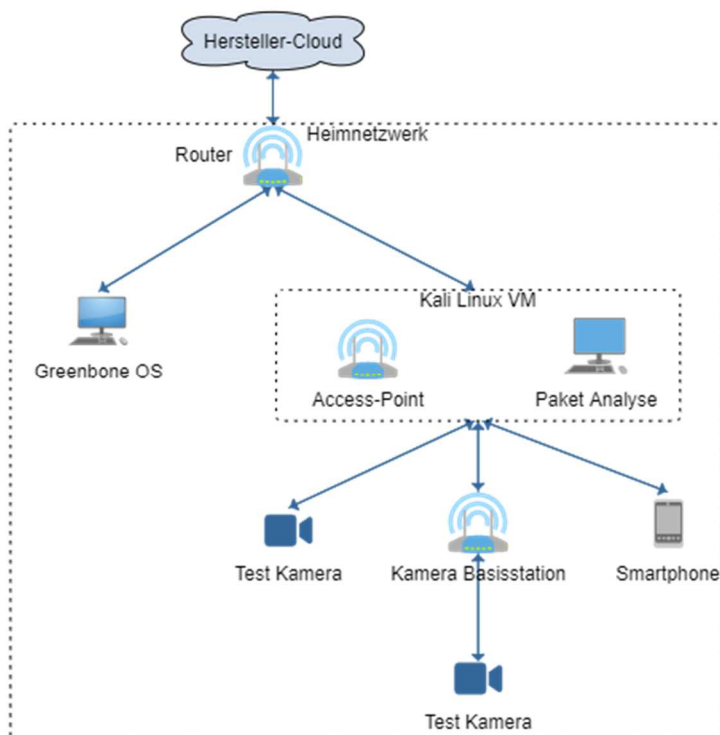


Abbildung 1 – Testaufbau

In einem üblichen Heimnetzwerk würden sich die zu testenden Kamerasysteme mit dem Router des Netzwerkes verbinden und so direkt mit den Cloud-Services des Herstellers kommunizieren. Im Test wurde ein zusätzliches Netzwerk, welches von einer virtuellen *Kali Linux*<sup>1</sup> Maschine kontrolliert wird, zwischengeschaltet. Dieser Aufbau erlaubt es, sowohl den Datenverkehr der Kameras in die Cloud als auch die Kommunikation der jeweiligen Kamera-App mit der Cloud und den Kameras zu überwachen.

Zusätzlich wurde eine virtuelle Maschine mit Greenbone OS und dem *OpenVAS Vulnerability Scanner*<sup>2</sup> verwendet, um die zu testenden Kameras und Basisstationen auf offene Ports und Schwachstellen zu überprüfen.

<sup>1</sup> <https://www.kali.org>

<sup>2</sup> <https://www.openvas.org>

## Testmethode

### Allgemeine Sicherheitsmerkmale

In diesem Abschnitt des Tests wurden die von den Kamerasystemen angebotenen Features auf ihre Sicherheitseigenschaften überprüft. Zu sicherheitsrelevanten Features zählen unter anderem Passwörter, Administration, Firmware, sowie das Teilen von Aufnahmen und Zugriffsberechtigungen mit anderen Nutzern. Informationen zu den vorhandenen Features wurden aus den jeweiligen Apps und Produktdokumentationen entnommen.

### Netzwerk- und Paketanalyse

Für die Prüfung des Sendeverhaltens der Kamerasysteme wurde der Datenverkehr über eine virtuelle Maschine mit Kali Linux umgeleitet. Auf diese Weise konnten die von den Kamerasystemen gesendeten Daten mittels des Analyse Tools *Wireshark*<sup>3</sup> aufgezeichnet werden.

Im ersten Schritt wurde überprüft, ob die Geräte oder die Smartphone-App unverschlüsselte Daten im Netzwerk oder zu Servern des Herstellers senden.

Im nächsten Schritt wurde mit Hilfe des Tools *mitmproxy*<sup>4</sup> ein Man-in-the-Middle-Angriff auf gesicherte Verbindungen zwischen der Smartphone-App und den Hersteller-Servern simuliert. Auf dem Smartphone wurde hierbei ein selbst erstelltes Sicherheitszertifikat installiert.

Das manipulierte Zertifikat wurde zuerst als User-Zertifikat installiert. Dieser Schritt kann von jedem Smartphone-User ohne Root-Rechte durchgeführt werden. Sofern eine Anwendung Sicherheitszertifikate korrekt überprüft, sollte ein solcher Manipulationsversuch leicht zu erkennen sein.

Anschließend wurde das Zertifikat mittels Root-Zugriff in den System-Zertifikatspeicher des Smartphones installiert. In diesem Speicher vertraut auch das Android-System dem Zertifikat. Durch Techniken wie z.B. „Certificate Pinning“<sup>5</sup> ist es Apps jedoch immer noch möglich, ein nicht vertrauenswürdiges Zertifikat zu erkennen.

Zuletzt wurden die Kamerasysteme mittels des Netzwerkscanners *nmap*<sup>6</sup> und des *OpenVAS Vulnerability Scanners* auf etwaige Schwachstellen untersucht, welche von Angreifern im lokalen Netz ausgenutzt werden könnten.

---

<sup>3</sup> <https://www.wireshark.org>

<sup>4</sup> <https://mitmproxy.org>

<sup>5</sup> <https://developer.android.com/training/articles/security-config#CertificatePinning>

<sup>6</sup> <https://nmap.org>

## Produkte im Test

Die folgenden Kamerasysteme wurden im Rahmen dieses Tests überprüft. Für alle Produkte wurde die zum Testzeitpunkt neueste Firmware- und App-Version verwendet.

Hersteller	Produkt	Firmware	App Version
<b>Anker</b>	Eufycam 2C	2.0.9.8h (Basisstation) 1.6.1 (Kamera)	1.7.4_581
<b>Arlo</b>	Pro 3	1.16.1.3_495_1a608c1 (Basisstation) 1.060.10.18_749_4b65ff8 (Kamera)	2.16.2_28010
<b>Blink</b>	XT2	2.13.18 (Sync Modul) 7.96 (Kamera)	6.0.10_524400
<b>Kami</b>	Dome X	4.3.0.0C_201909250959	2.1.3_20200417
<b>Nest</b>	Cam IQ Indoor	4720014	5.50.0.7
<b>Ring</b>	Stick Up Cam	22.05.2020 (Versionsnummer nicht angezeigt)	3.26.0

## Testergebnisse

Um eine bessere Übersicht über die Testergebnisse zu bieten, werden in diesem Abschnitt die gesammelten Informationen zunächst in einer Tabelle zusammengefasst und anschließend die dargestellten Ergebnisse in Textform detaillierter diskutiert.

## Symbole

Die folgenden Symbole wurden für die Bewertung der Testkriterien verwendet:

Symbol	Bedeutung
●	„Ja“, Funktion vorhanden
◻	„Teilweise“, Funktion eingeschränkt verfügbar
○	„Nein“, Funktion nicht vorhanden
<b>k.A.</b>	Keine Angaben – konnte nicht überprüft werden – siehe Detailergebnisse

	Anker Eufycam 2C	Arlo Pro 3	Blink XT2	Kami Dome X	Nest Cam IQ	Ring Stick Up Camera
<b>Login/Passwort</b>						
Prüfung der Passwortstärke	?	●	●	●	●	?
Passwortanforderungen	8-20 Zeichen	8 Zeichen Groß- /Kleinschreibung Zahl Sonderzeichen	8 Zeichen Groß- /Kleinschreibung Zahl Sonderzeichen	8-16 Zeichen Groß- /Kleinschreibung Zahl	8 Zeichen Buchstaben Zahl Sonderzeichen	8 Zeichen
Zwei-Faktor-Authentifizierung (2FA)	○	●	○	○	●	●
Lockout nach gescheiterten Anmeldeversuchen	●	●	●	○	? <sup>7</sup>	○
<b>Wi-Fi Verbindung</b>						
Warnung bei ungesichertem Netzwerk	k.A.	k.A.	●	●	○	○
<b>Firmware</b>						
Update während Setup	●	●	●	●	k.A.	●
Automatische Updates	●	●	●	●	●	●
Manuelles Update verfügbar	●	●	●	●	○	●
Sicherer Firmware Download (HTTPS)	○	●	●	○	k.A.	●
<b>Videoübertragung</b>						
Gesicherte Übertragung von/zu Cloud	●	●	●	?	?	●
<b>Speicherung</b>						
Cloud	●	●	●	●	●	●
Speicherdauer in Cloud konfigurierbar	○	○	●	○	○	○
Lokal	●	●	○	○	○	○
NAS	●	○	○	○	○	○
<b>App</b>						
Benutzerkonto beim Hersteller notwendig	●	●	●	●	●	●
Angefragte Berechtigungen sinnvoll	●	●	●	●	●	●
Logout von App	●	●	●	●	●	●
SSL Zertifikat Überprüfung	●	●	●	○	●	●
SSL Zertifikat Überprüfung (System)	●	●	○	○	○	●

<sup>7</sup> Anmeldung mit Google-Account – Captcha nach zu vielen Anmeldeversuchen

	Anker Eufycam 2C	Arlo Pro 3	Blink XT2	Kami Dome X	Nest Cam IQ	Ring Stick Up Camera
<b>Geteilter Zugriff</b>						
<b>Andere App-User</b>						
Administration	●	●	○	○	●	☒ <sup>8</sup>
Live-Stream	●	●	○	●	●	●
Aufnahmen	●	●	●	●	●	●
Admin/Nicht-Admin-Zugriff konfigurierbar	●	●	k.A.	k.A.	○	○
<b>Öffentlicher Zugriff via Browser</b>						
Zugriff auf Live-Stream konfigurierbar	○	○	○	○	●	○
Passwortschutz konfigurierbar	○	○	○	○	●	○
<b>Weitere Sicherheitstests</b>						
OpenVAS: keine Schwachstellen	●	●	●	●	●	●
Offene Ports	554 (RTSP) <sup>9</sup>	○	53 (DNS)	○	○	○

<sup>8</sup> Nicht alle Einstellungen sind für andere App-User verfügbar<sup>9</sup> Nur geöffnet, wenn die entsprechende Option in der App aktiviert wurde



## Detailergebnisse

### Setup & Login

Beim Erstellen eines neuen Benutzerkontos erlauben die Apps der **Anker Eufycam 2** und der **Ring Stick Up Camera** das Verwenden von unsicheren Passwörtern. Bei diesen Apps können einfach zu erratende Passwörter, wie z.B. „passwort“, verwendet werden, welche nur wenig Schutz gegen unautorisierten Zugriff auf das Benutzerkonto bieten.

Bei der App der **Ring Stick Up Camera** kann dieser Schwachpunkt jedoch durch das Einrichten einer Zwei-Faktor-Authentifizierung (2FA) über einen per SMS zugesendeten Sicherheitscode kompensiert werden. Selbst wenn der Nutzer die 2FA nicht aktiviert, so muss er nach jedem Login einen per E-Mail versandten Sicherheitscode eingeben, um die Funktionen der App nutzen zu können. Auch die Apps der **Arlo Pro** und der **Nest Cam IQ** bieten diese zusätzliche Sicherheitsfunktion an – letztere indirekt über die Anmeldung mittels Google-Account.

Die Apps der **Kami Dome X** und der **Ring Stick Up Camera** bieten kein Lockout an, wodurch beliebig viele Anmeldeversuche möglich sind. Bei der **Nest Cam IQ** können sich neue Nutzer nur mehr über ihren Google Account anmelden. Bei zu vielen gescheiterten Anmeldeversuchen wird die Eingabe eines Captcha-Codes erforderlich. Die Apps der restlichen Kameras sperren nach einigen fehlgeschlagenen Anmeldeversuchen den Benutzeraccount für eine gewisse Zeit. Diese Methode, wie auch die Captcha-Methode, machen ein erraten des Passworts durch einen Brute-Force Angriff unpraktikabel.

Beim ersten Einrichten der Kameras lassen sich die **Ring Stick Up Camera** und die **Nest Cam IQ** ohne Warnung mit einem ungesicherten Drahtlosnetzwerk verbinden. Auf Grund der relativ hohen Reichweite von Wi-Fi-Netzwerken könnten somit auch Nachbarn Daten, welche unverschlüsselt im lokalen Netzwerk gesendet werden, mitlesen.

Die Kamerasysteme **Anker Eufycam 2C** und **Arlo Pro 3** verwenden Basisstationen, welche über eine Kabelverbindung mit dem Router des Heimnetzwerkes verbunden werden. Dadurch entfällt dieser Testpunkt bei diesen Geräten. Die Basisstationen dieser beiden Systeme, wie auch jene der **Blink XT2** bauen ein eigenes Drahtlosnetzwerk auf, mit dem sich die Kameras verbinden. Die so erstellten Netzwerke sind jeweils mit WPA2 vor unbefugtem Zugriff gesichert.

### Firmware

Mit Ausnahme der **Nest Cam IQ** führen alle Kamerasysteme nach dem ersten Einrichten ein für den Benutzer sichtbares Update der Gerätefirmware durch. Laut Produktdokumentation halten alle Systeme die Firmware über automatische Updates aktuell. Dies verhindert, dass Nutzer für längere Zeit Firmware mit potenziellen Sicherheitslücken verwenden.

Die Firmware der **Kami Dome X** und der **Anker Eufycam 2C** werden unverschlüsselt über eine HTTP Verbindung heruntergeladen, was ein potenzielles Sicherheitsrisiko durch manipulierte Firmware darstellt.

Source	Destination	Protocol	Length	Info
192.168.0.46	47.254.187.24	HTTP	284	GET /yifirmware/smarthomecam/familymonitor-y32-manual/4.3.0.0C_201909250959restore.zip
47.254.187.24	192.168.0.46	TCP	60	80 → 47528 [ACK] Seq=1 Ack=231 Win=30720 Len=0

Abbildung 2 -- Kami Dome X: Unverschlüsselter Download der Firmware

Source	Destination	Protocol	Length	Info
192.168.0.88	52.219.72.132	HTTP	213	GET /security/8312d3e2-2388-4a92-91b4-09448235ea47_eufy_2.0.9.8h_20200509.img
52.219.72.132	192.168.0.88	HTTP	1095	HTTP/1.1 200 OK

Abbildung 3 -- Anker Eufycam 2C: Unverschlüsselter Download der Firmware



### Videoübertragung

Alle Kamerasysteme senden Videoaufnahmen ausschließlich verschlüsselt an ihre Cloud-Server.

**Kami Dome X** sendet Aufnahmen über das HTTP-Protokoll und verwendet eine proprietäre Verschlüsselung für die gesendeten Daten. Obwohl diese Vorgehensweise nicht unbedingt ein Sicherheitsproblem darstellen muss, so gleicht sie eher einem „Security through Obscurity“ Ansatz. Die Verwendung von etablierten verschlüsselten Übertragungsverfahren wie HTTPS/TLS wäre hier zu bevorzugen. Die Live-Übertragung des Video-Streams zur Smartphone App erfolgt über eine, ebenfalls proprietär verschlüsselte, UDP Verbindung.

Source	Destination	Protocol	Length	Info
10.42.0.69	47.254.187.8	HTTP	630	POST /
47.254.187.8	10.42.0.69	HTTP	360	HTTP/1.1 200 OK
47.254.187.8	10.42.0.69	HTTP	79	HTTP/1.1 100 Contin
47.254.187.8	10.42.0.69	HTTP	79	HTTP/1.1 100 Contin

Abbildung 4 – Kami Dome X: Übertragung von Aufnahmen über HTTP

**Nest Cam IQ** verwendet für die Übertragung von Videos von der Kamera zur Cloud die veraltete Version 1.0 des Verschlüsselungsprotokolls TLS, welche von gängigen Web-Browsern als unsicher eingestuft wird. Ein Upgrade auf eine neuere Version (1.2/1.3) ist hier empfehlenswert. Bei der Übertragung von der Cloud zur Kamera-App werden hingegen die neueren Protokollversionen für den Videodownload verwendet.

Source	Destination	Protocol	Length	Info
10.42.0.65	35.195.33.221	TLSv1	153	Client Hello
35.195.33.221	10.42.0.65	TCP	66	443 → 47338 [
35.195.33.221	10.42.0.65	TCP	1474	443 → 47338 [
35.195.33.221	10.42.0.65	TLSv1	265	Server Hello,

Abbildung 5 – Nest Cam IQ: Verbindung von Kamera zu Cloud über TLS 1.0

### Speicherung

Lokale Speicherung von Videoaufnahmen ermöglicht Nutzern volle Kontrolle über die aufgenommenen Daten, ohne sich auf den vertrauensvollen Umgang der Daten durch den Hersteller verlassen zu müssen. Nur zwei der getesteten Kamerasysteme erlauben es, aufgenommene Videos lokal zu speichern.

An die Basisstation der **Arlo Pro 3** kann ein USB-Speicher angeschlossen werden, um Videoaufnahmen auf diesem anstatt in der Cloud zu speichern.

In der Basisstation der **Anker Eufycam 2C** ist bereits ein 16GB großer Speicher integriert, der für die Speicherung von Aufnahmen verwendet werden kann. Zusätzlich können Aufnahmen auch über RTSP an einen Netzwerkspeicher im lokalen Netzwerk des Nutzers (NAS) gesendet werden. Es werden hierbei nur Ereignisaufnahmen übertragen, welche z.B. durch Bewegungserkennung ausgelöst werden. Obwohl das RTSP-Protokoll das Sichern des übertragenen Streams mittels Passworts unterstützt, kann in der App kein Passwort für die Übertragung festgelegt werden. Dadurch kann jeder Nutzer, der sich im lokalen Netzwerk befindet, die übertragenen Aufnahmen mitlesen.

### App

Alle Apps der getesteten Kameras fordern nur jene Berechtigungen am Smartphone an, welche für die Funktionsweise der App notwendig sind.

Bei einigen Apps wäre es jedoch wünschenswert, wenn diese den Benutzer weitere Informationen zur Verwendung der angefragten Berechtigungen geben würden. So fragen z.B. die Apps von **Kami Dome X** und **Anker Eufycam 2C** die Standort-Berechtigung für das Aufsetzen der Kameras an. Jedoch geht aus dem Setupvorgang nicht klar hervor, warum diese Berechtigung benötigt wird.

Auch die App der **Ring Stick Up Camera** liefert keine genauere Erklärung für die angefragte Standort-Berechtigung. Sie informiert den Nutzer jedoch zumindest, dass die Berechtigung nur während des Setups benötigt wird und nachher wieder zurückgezogen werden kann.

Um einen erfolgreichen Man-in-the-Middle Angriff auf gesicherte TLS-Verbindungen durchzuführen, ist es normalerweise nötig, den Client (in unserem Fall das Smartphone mit der Hersteller-App) davon zu „überzeugen“, ein vom Angreifer erstelltes Sicherheitszertifikat als vertrauenswürdig einzustufen. Zum Entschlüsseln der gesendeten App-Daten der **Kami Dome X**, ist dieser Schritt jedoch nicht erforderlich – die App scheint die Überprüfung der TLS-Zertifikate zu überspringen und akzeptiert ohne Warnung alle Zertifikate.

```
"isNew": true,  
"message": "",  
"model": "17",  
"name": "Kami Camera",  
"nickname": "YI_XXXXXX",  
"online": true,  
"password": "XXXXXXXXXXXXXXXXXXXX",  
"share": false,  
"state": 1,  
"type": 2,  
"uid": "XXXXXXXXXXXX"
```

Abbildung 6 -- Kami Dome X: Account- und Kamerainformationen

Abbildung 6 -- Kami Dome X: Account- und Kamerainformationen zeigt einen Ausschnitt eines Datenpakets, welches durch einen Man-in-the-Middle Angriff ausgelesen werden konnte. Es werden unter anderem der Account-Name, die Identifikationsnummer der verbundenen Kamera sowie ein Passwort-Hash übertragen. Da die Videoübertragung eigens verschlüsselt ist, konnte diese auch mit Hilfe dieser Informationen nicht entschlüsselt werden. Trotzdem stellt die fehlende Zertifikatsüberprüfung ein Sicherheitsrisiko dar.

Auch mit einem, als vertrauenswürdig markiertem, Zertifikat verweigerten die Apps der **Anker Eufycam 2C**, **Ring Stick Up Camera** und **Arlo Pro 3** den Zugriff auf den Nutzeraccount und die Kameras, wodurch im Test kein Man-in-the-Middle Angriff auf übertragenen Daten dieser Apps möglich war.

Die App der **Nest Cam IQ** und der **Blink XT2** führen eine Ordnungsgemäße Prüfung der Sicherheitszertifikate durch, vertrauen jedoch den Zertifikaten des Systemspeichers. Eine genauere Prüfung der Zertifikate wäre hier empfehlenswert.

Geteilter Zugriff

Die Apps aller Hersteller erlauben es, anderen Benutzern zumindest eingeschränkten Zugriff auf Kameradaten zu ermöglichen.

Außer bei der **Kami Dome X** und der **Blink XT2** können auch Administrator-Nutzer angelegt werden. Dies erlaubt es anderen Nutzern auch die Konfiguration der Kameras, wie z.B. Video- und Audioeinstellungen, zu verändern.

Die Apps der **Anker Eufycam 2C** und der **Arlo Pro 3** erlauben es außerdem, Benutzern verschiedene Rechte zuzuweisen. So können Benutzer entweder nur Zugriff auf Videoaufnahmen oder Vollzugriff erhalten.

In der App der **Nest Cam IQ** können Nutzer den Live-Stream der Kamera veröffentlichen. Der Stream kann dann auch ohne App über einen Link in einem Browser geöffnet werden. Der Zugriff auf diesen Stream kann zusätzlich mit einem Passwort geschützt werden.

Weitere Sicherheitstests

Keine der Kameras oder Basisstationen nutzt Dienste, welche laut den Ergebnissen des OpenVAS Scanners angreifbare Schwachstellen aufweisen. Im lokalen Netzwerk sind keine kritischen Ports standardmäßig geöffnet.

## Fazit

Bei der **Anker Eufycam 2C** wurde ein Sicherheitsmangel festgestellt. Der unverschlüsselte Download von Firmware-Updates könnte eine Manipulation der Gerätefirmware ermöglichen. Die Smartphone-App akzeptiert zwar schwache Passwörter für den Benutzeraccount, jedoch verhindert nach wenigen fehlgeschlagenen Anmeldeversuchen eine Accountsperre das Erraten des Passworts. Durch die Möglichkeit der lokalen Aufnahme können Nutzer die Kamera auch verwenden, ohne ihre Aufnahmen an die Cloud-Server des Herstellers zu senden. Bei der lokalen Speicherung ist der interne Speicher der Basisstation zu bevorzugen, da die Übertragung auf einen lokalen Netzwerkspeicher nicht verschlüsselt ist.

Beim **Arlo Pro 3** Kamerasystem konnten im Test keine Sicherheitsmängel festgestellt werden. Nutzer können Videoaufnahmen auch lokal abspeichern, ohne sie an die Cloud-Server des Herstellers zu senden.

Das **Blink XT2** Kamerasystem schnitt im Test größtenteils positiv ab. Die Überprüfung von Sicherheitszertifikaten durch die Smartphone App könnte jedoch verbessert werden. Ansonsten wurden keine weiteren Sicherheitsmängel festgestellt.

Bei der **Kami Dome X** wurden im Test einige Sicherheitsmängel festgestellt: Die Gerätefirmware wird durch die App der Kamera unverschlüsselt heruntergeladen. Bei der Übertragung von Videoaufnahmen zu den Cloud-Servern des Herstellers setzt die Kamera auf eigene Verschlüsselungsmethoden, anstatt bewährte Übertragungsverfahren wie HTTPS/TLS einzusetzen. Da die App der Kamera keine Überprüfung der Sicherheitszertifikate durchführt, ist ein Man-in-the-Middle Angriff auch ohne Installation des manipulierten Zertifikates auf dem Smartphones des Opfers möglich.

Die **Nest Cam IQ** schnitt im Test größtenteils positiv ab. Ein Manko ist die Verwendung des veralteten Übertragungsprotokolls TLS Version 1.0 für die Übertragung der Video-Daten von der Kamera zur Hersteller-Cloud. Die Überprüfung von Sicherheitszertifikaten durch die Smartphone App könnte verbessert werden.

Die **Ring Stick Up Camera** schnitt im Test weitgehend gut ab. Die einzigen Kritikpunkte sind die Erlaubte Vergabe von schwachen Passwörtern für Nutzer-Accounts und das Fehlen eines Lockout-Mechanismus bei zu vielen fehlgeschlagenen Anmeldeversuchen. Ansonsten konnten keine Sicherheitsmängel festgestellt werden.



## Copyright and Disclaimer

This publication is Copyright © 2020 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives  
(June 2020)