IP-Kameras: Firmware ohne Hintertür

Inhaltsverzeichnis

1. Allgemein....1
1.1. Begriffe, Protokolle....1
1.2. Rechtliches....3
1.3. Sicherheits-Probleme....3
1.4. Praktische Hinweise....5
1.5 Ausblick....5
2. Alternative Firmware für TENVIS TH692....6
2.1. Firmwareupdate....6
2.2. Konfiguration der Firmware....7
3. Sicherung von Kameras ohne Modifizierung der Firmware....13

1. Allgemein

1.1. Begriffe, Protokolle

Eine Überwachungskamera kann vielfältig eingesetzt werden: Abschreckung von Gelegenheitsdieben/Einbrechern, Beweissicherung, Ursachenforschung (Parklatzraudys, Marder..) oder einfach nur aus Neugier. Moderne Überwachungskameras sind mittlerweile auch kleine technische Wunderwerke: Nicht nur eine exzellente Auflösung bei Tageslicht, wie sie selbst vor Jahren noch undenkbar war, sondern auch hervorragende Bildqualität in der Nacht haben die Kameras, zudem eine automatische Bewegungserkennung, eine Fülle von unterstützenden Protokollen, die von „live“-Bildern über den automatischen Email Versand bis zu P2P reichen, Fernsteuerung von Mikrofon, Schwenkbereich und Zoom...

Seit der Jahrtausendwende hat mit den fallenden Preisen dieser Technik ein wahrer Boom auch den privaten Sektor erreicht. Dieses Dokument soll den privaten Nutzer ein wenig durch den „Dschungel“ der aktuellen Protokolle führen, Tendenzen und Risiken des Überwachungswahns aufzeigen und nicht zuletzt auch eine konkrete Alternative für ambitionierte Bastler anbieten.

Nun zu den Begriffen und Protokollen:

Begriff/Protokoll	***Was ist das?***	***Vorteile***	***Nachteile***
IP	„Internet protocol“ - Verbindung erfolgt paketbasiert über Internet/Intranet	Einheitliche (Hardware-) Netzwerktopologie für alle Komponenten ohne spezielle Videoleitungen	Eventuell zusätzliche Stromversorgung notwendig
LAN	Kabelbasierte Übertragung	Unempfindlich gegen Störungen, Stromversorgung integrierbar (PoE)	Erhöhter Installationsaufwand
WLAN	Drahtlose Übertragung (immer mit mind. WP2-Verschlüsselung!)	Geringer Installationsaufwand	Leicht von außen störbar durch Jammer o.ä.
	• a: 5 GHz, max. 54 Mbits/s • b: 2.4 GHz, max. 11 Mbits/s • g: 2.4 GHz, max. 54 Mbits/s • n: 2.4 & 5 GHz, max. 600		

Begriff/Protokoll	*Was ist das?*	*Vorteile*	*Nachteile*
	Mbits/s • ac: 5 GHz, max. 1.3 Gbits/s		
HD	Bildauflösung besser als 640x480 (veraltet)	Höhere Detailschärfe (hängt aber auch vom Objektiv ab) Identifizierung von Personen, Nummernschildern, Aktionen	Höheres transferiertes Datenvolumen, erhöhter Speicherplatz Alarmauslösung möglicherweise häufiger teurer
	• 720p (1280×720 Pixel) bzw. 1,3Megapixel; Dateigröße: ca. 100kB je jpg-Bild	Ab ca. 2013 preiswerter Standard im privaten Bereich	Max. 5m breiter Bereich überwachbar
Full-HD	• 1080p (1920x1080 Pixel) bzw. 2 Megapixel; Dateigröße ca. 250kB je jpg-Bild	Ab ca. 2015/6 preiswerter Standard im privaten Bereich	Max. 7m breiter Bereich überwachbar
4K/UltraHD/UHD	• 2160p (3840 x 2160 Pixel) bzw. 8,3 Megapixel; Dateigröße >1,5MB je jpg-Bild	Standard in professioneller Videoüberwachung	4K-Monitor notwendig, hohe Datenraten, speicherintensiv, noch sehr teuer. Bei 8MP sind das mehr als 20 GByte Video pro Stunde!
H.264	Standard für die Videokompression (MPEG-4/AVC bzw. Advanced Video Coding)	Hohe Datenkompression bei Videoübertragung	
PoE	Power over Ethernet – Stromversorgung per LAN	Nur ein Kabel notwendig	Kamera und Netzwerk-topologie muss PoE unterstützen, noch teuer – ist aber im kommen
Integrierte IR-Beleuchtung	LEDs, die den Überwachungsbereich nachts beleuchten	preiswert	Jede Menge Fehlalarme bei ungünstigem Einbau/ Wetterlagen Alternative: externe IR-Beleuchtung
Blickwinkel	Sichtbarer Bereich (üblich sind 30..80 Grad)		
Zoom, Zoomfaktor, Motorzoom	Hinweise zur Bildvergrößerung	Nur optischer (hardware-) Zoom bringt Detailschärfe in ausgewählten (einstellbaren) Bereichen	Möglicherweise nur Marketingwerte
Feste Brennweite, fixierte Blende	Regulierung der Belichtungszeit durch Shutter	Einfache (ältere) Technik, ist in jeder Kamera eingebaut	Im Außenbereich: Gefahr des Smear-Effekts (Verbrennen des Chips)
Auto-Iris	Automatische Regulierung der Belichtung per Blende (zusätzlich zum Shutter)	Im Außenbereich: keine Gefahr durch Smear-Effekt	
Infrarot-Objektiv	• Tag/Nacht Objektiv	Unverfälschte Farben am Tag	teuer
	• I/R vergütetes Objektiv	preiswert	Verfälschte rote Farben am Tag
IR-Sperr-Filter (IR-Cut)	Fernhalten von UV-Strahlen vom Kamerachip	Bei Außenkameras: Verlängerung der Lebensdauer	
Autofokus	Automatisches „Scharfstellen“		Bei Überwachungskameras unnötiger „Luxus“
Outdoor	Nicht geschützter Begriff für „Außeneinsatz“, besser ist die Angabe von IP x5/ IP x6		
Alarmauslösung	Eventtrigger bei Bewegungs-		

Begriff/Protokoll	*Was ist das?*	*Vorteile*	*Nachteile*
	erkennung im Bild und/oder bei Geräuscherkennung		
Motion-Control, Bewegungserkennung	Bei Änderung des Bildinhaltes (Schwelle und Bereich i.d.R. Einstellbar) wird Alarm ausgelöst	Super Funktion!	Jede Menge Fehlalarme bei ungünstigem Einbau/ Wetterlagen (besonders nachts)
IP-Adresse	Adresse der Kamera, üblich ist eine im „Privat-“ Bereich 192.168.x.x		
dhcp	Die IP-Adresse wird automatisch (vom Router/PC) vergeben	Schnellere Installation	Möglicherweise nach nächstem Routerstart andere Adresse → Lesezeichen funktionieren nicht mehr
DDNS (zusammen mit Portfreischaltung/Port Mapping)	dynamisches Domain-Name-System (somit erhält das Gerät immer die gleiche Internet-Adresse)	Kamera ist aus dem Internet erreichbar	Kann u.U. auch von „Fremden“ genutzt werden → sichere Passwörter notwendig!
Anzahl Videostream	Mehrere Streams werden gleichzeitig an verschiedene Empfänger übertragen. Max. Anzahl hängt von Prozessor-leistung der Kamera ab		Eventuell hohe Bandbreite erforderlich Alternativen: Multicast, RTSP, P2P
Multicast, RTSP	Kompliziertes Übertragungsprotokoll: kurz gesagt - einer sendet, viele empfangen (Port554)	Bessere Ausnutzung der Technik, wenn viele Empfänger des live-Bildes (Streamen via. Multicast, RTSP oder RTSP-over-HTTP)	Für normale Nutzer viel zu kompliziert, Einsatz spezifischer Software not-wendig, dadurch potentiell unsicher
ONVIF	Verbindungsprotokoll: offener Industriestandard, Grundlage des „live“ Bildes	Kombination Kamera – Standard-PC/Browser bis hin zur Bewegungssteuerung ist problemlos möglich	
P2P	Verbindungsaufbau erfolgt per UID und über Server eines Anbieters. Die Datenübertragung selbst ist „Point to Point“	Einfache Installation, direkte Datenübertragung ins Internet, Smartphone geeignet	Sicherheitsproblem: Zugangsdaten werden vom Anbieter verwaltet, potentiell hackbar

1.2. Rechtliches

Die Rechtsvorschriften in Deutschland begrenzen den Handlungsspielraum für den Einsatz von Überwachungskameras: Eine Nutzung von Überwachungskameras im privaten Raum ist grundsätzlich nur dann erlaubt, so lange Aufzeichnung und Bildausschnitt nur das Privatgelände abbilden. Unbeteiligte auf öffentlichen Wegen dürfen also nicht zu sehen sein. Gab es bereits Straftaten, so stellt das Ordnungsamt ggf. Ausnahmegenehmigungen aus. Ein Hinweisschild auf die Videoüberwachung ist für den privaten Bereich zwar nicht zwingend vorgeschrieben, hat aber in der Praxis durchaus eine abschreckende Wirkung.

1.3. Sicherheits-Probleme

Eigentlich ist alles ganz einfach: Der Admin legt fest und die Kamera macht ;-)

In der Praxis zeigen sich aber die Tücken der IT-Technik. Eine IP-Kamera soll 100 % sicher vor fremden Zugriff sein, sie darf also nicht von außen „übernommen“ werden. Damit müssen also alle relevanten Einstellungen ausschließlich in der Kamera oder im lokalen (sicherem) Netz erfolgen.

Den Datenstrom unkontrolliert in das Internet senden zu lassen ist eine Grauzone. Fremde könnten so Einblick erhalten, können aber an den Einstellungen nichts ändern.

Wie die Tabelle unter 1.1 bereits zeigt, sind die Protokolle Multicast, RTSP, P2P deshalb mit Vorsicht zu genießen. Insbesondere bei P2P meldet sich die Kamera regelmäßig auf fremden Servern – was bei gehackten Servern natürlich zum Problem werden könnte. Nebenbei hat der Betreiber (und die entsprechenden Geheimdienste) nicht nur die Metadaten zur Verfügung. Man muss sich letztlich entscheiden, ob man die Sicherheit zugunsten der Bequemlichkeit aufgibt. Es ist natürlich verlockend immer von überall per Smartphone auf die Bilder zuzugreifen und sei es, nur um zu sehen, ob die Kamera online ist.

Aber auch der normale Video-Datenstrom, der per ONVIF bei praktisch jeder Kamera unverschlüsselt gesendet wird gelangt bei Portfreigabe im Router ins Internet. Wenn man sich sicher ist, dass der Datenstrom nach gewisser Zeit (nach einem Passwort gesteuertem Zugriff) versiegt, kann eigentlich nur ein „man in middle“ die Daten abgreifen. Besser ist aber generell auf einen VPN-Kanal für die Verbindung zur heimischen Domäne zurückzugreifen.

Die sicherste Variante ist deshalb:

- „live“ Video der Kamera nur im lokalen Netz oder aber per zugeschaltetem VPN Kanal aus dem Internet sehen. Bei direkter Übertragung ins Internet sollte der Zugriff und die Übertragung per SSL oder anderer Verschlüsselung geschehen (was billige Cams aber noch nicht können), eine Portweiterleitung im Router muss konfiguriert werden.
- Die Bewegungserkennung der Kamera für einen automatischen FTP-Upload auf einen eigenen NAS-Server bzw. beim Projekt „Hauscomputer“ auf den Stick der Haussteuerung im 192.168.x.x -Netz nutzen. Dabei muss man berücksichtigen, dass bei Außenkameras und ungünstigen Wetterbedingungen (Regen, Schnee, Sturm, Nebel) erhebliche Fehlauslösungen auftreten können. Erfolgt der Upload dagegen ins Internet (eigener Provider) oder zu einem Cloud-Dienst, so ist eine Verschlüsselung der Zugangskennung **und** des Datenstromes Pflicht
- Bei Alarmauslösung eine (unempfindliche) Einstellung für den automatischen (und verschlüsselten) Email-Versand nutzen. Es soll schon vorgekommen sein, dass eine Kamera mehr als 500 (!) Mails je Stunde gesendet hat
- Alle anderen Protokolle sollten abgeschaltet werden, es sei denn, man weiß was man tut ;-)
- Es gibt noch ein Restrisiko: der Urheber der Firmware baut oft noch „Hintertüren“ in die Kamera ein, warum auch immer. http://www.spiegel.de/netzwelt/netzpolitik/bnd-skandal-netbotz-baut-offenbar-hintertueren-in-seine-kameras-a-1114252.html Dieses Risiko lässt sich nur durch alternative Firmware beheben
- Den Zugang zur Kamera nur mit eigenen Passwörtern erlauben (keine Werkseinstellungen!)

1.4. Praktische Hinweise

- Bei Außenkameras mit integrierten IR-LEDs läßt es sich nicht verhindern, dass Partikel in der Luft nachts zu Fehlalarmen führen – die intensive Anstrahlung der Teilchen auf kurzer Distanz ist daran schuld. Selbst Nebeltröpfchen reflektieren intensiv infrarotes Licht. Zudem regelt der interne Videoverstärker im Dunkeln auf Maximum. Beheben lässt sich dieser Effekt nur durch den Einsatz externer IR-Beleuchtung, die in einem ausreichenden Abstand montiert werden muss. Die internen LEDs sind abzuschalten.

  Ein für das menschliche Auge noch klarer Nachtblick (leichter Nebel, Sichtweite 150 m) macht der Kamera bereits Probleme und führt zum Alarm (da waren keine Insekten!):

  Auch Spinnweben (besonders im Herbst) führen oft zum Alarm.
- Bei der Konfiguration von Email-versand ist immer (auch beim ersten Mal) eine Verschlüsselung einzustellen (z. B. STARTTLS)
- Auch wenn die Angabe „Outdoor“ auf der Kamera steht, ein zusätzlicher Wetterschutz ist immer sinnvoll.

1.5 Ausblick

Zukünftige Überwachungskameras werden billiger, haben eine höhere Auflösung und immer weitergehende Übertragungsprotokolle. Hier den Überblick zu behalten dürfte schwierig werden. Ich denke, bei 4-8Megapixel ist eine Grenze erreicht. Höhere Auflösungen sind für Beweissicherungen nicht notwendig, die Fehlauslösung von Alarmen steigt eher und der benötigte Speicherplatz und die Folgekosten auch. Das Problem der Sicherheit wird öffentlich mehr diskutiert werden und wahrscheinlich technische Konsequenzen haben. Z. B., dass man einzelne Protokolle im Setup der Kamera definitiv Ein- und Ausschalten kann. Eine Zertifizierung billiger Kameras für den privaten Bereich wird es aber wohl nicht geben. Daneben wird aber künftig PoE auch bei preiswerten Kameras Einzug halten und es wird manche Überraschung geben – man denke nur an 3D …

2. Alternative Firmware für TENVIS TH692



Die Kamera TENVIS TH692 ist eine preiswerte chinesische HD Kamera (1280 × 720) mit integrierten IR-LEDs. Der Hersteller TENVIS ist in Shenzhen beheimatet (http://de.hktdc.com/manufacturers-suppliers/TENVIS-Technology-Co-Ltd/en/1X08ZH6F/). Bildqualität bei Tag und Nacht sind ausgezeichnet. Eine integrierte Bewegungserkennung lässt sich komfortabel in 4 Bereichen einstellen. Die Firmware unterstützt auch eine Reihe von Protokollen:

H.264, FTP, Email, P2P, ONVIV, Dual-Stream

Quelle: http://www.netzwerk-kamera-infothek.de/amazon-produkt/tenvis-th692-ip-kamera

Die TH692 ist als Einstiegskamera für Überwachungszwecke hervorragend geeignet, wenn da nicht ein Problem wäre: Aus gegebenen Anlass wurde die Netzwerkkommunikation analysiert und eine Reihe nicht autorisierter Datenverbindungen der Kamera festgestellt. Daraufhin wurde die Firmware (**B18TV_V17.1.1.2.2-20151217(720P.factory.0A0.38 板).pkg**) „zerlegt“ und gründlich untersucht. Das Ergebnis ist folgendes: In der Firmware finden sich eine Reihe von Netzwerkadressen, die einerseits für die programmierbaren P2P und DDNS Verbindungen notwendig sind, anderseits aber auch eine komplette Server-Basis enthält mit tief in den Programmen verwurzelten vorerst unklaren Adressen. Für P2P sind in der originalen Firmware z. B. die Server der taiwanesischen Firma ThroughTek implementiert, die mit Amazon zusammenarbeitet. Daneben gibt es aber auch Adressierungen zu shenzen, dropbox, icloud, baidu, Google und QQ.

Im nächsten Schritt wurden alle diese (nicht benötigten) Adressen entfernt oder (wo das nicht möglich war) mit Adressen im Bereich 192.168.x.x ersetzt. Im Ergebnis funktionieren ONVIV, Email und FTP nach wie vor problemlos; Multicast, P2P und alles andere sind dagegen abgeschaltet. Auch der erneut gemessene Datenverkehr ist jetzt „sauber“.

Die modifizierte Firmware wurde mit einem neuen Logo versehen und die FTP-Alarmauslösung wurde beschleunigt. Die neue Firmware heißt nun: **Firmware TH692 17.1.1.2.2d.pkg**, wobei die Softwareversion 17.1.1.2.2d nun natürlich auch im Web-Ftrontend der Kamera ersichtlich ist.

2.1. Firmwareupdate

Für die Konfiguration der Kamera benötigt man einen Browser im gleichen Netz und ein Netzwerkkabel zur Kamera (WLAN ist nach dem Update abgeschaltet). Das Web-Frontend der Kamera öffnet man mit der Adresse 192.168.x.x in der Adressleiste. Die aktuelle Adresse weiß der Router. Für ein „live“-Bild ist unter Windows u.U. ein zusätzliches OCX Modul zu installieren.

Unter Linux geht es (bisher noch) nicht.

Im Kamera-Setup findet sich unter „Sonstiges“ der Punkt „System-Upgrade“:



Hier ist zunächst mit „öffnen“ die neue Firmware von der Projekt-DVD hochzuladen (Ordner ../Programme/Kameras/TENVIS TH692/Firmware TH692 17.1.1.2.2d.pkg) und dann mit „Upgrade“ zu starten. Im gleichen Ordner findet sich auch die originale Firmware, sowie die TENVIS-eigene Übersicht aller gültiger Firmware:

Model Number	Hardware	Firmware	Latest Firmware	Download Number
TH692	9.10	0.9.3.X / 9.1.1.1.X	16.1.16.1.1.4	42
	1.0.0.1	17.1.1.1.X.X.X	17.1.1.1.3.0	43
		17.1.1.2.X.X.X	17.1.1.2.2	44

(Stand Februar 2017)

Das Upgrade lädt zunächst die Firmware in die Kamera, prüft die Gültigkeit und installiert sie dann. Achtung: Hier endet die Gewährleistung!

Anschließend meldet sich die neue Firmware mit der Passwortabfrage:

Benutzer: admin

Passwort: admin

Warum auch immer, diese Eingaben muss man dreimal machen, dann erst kommt ein Fenster, dass zum Passwortwechsel auffordert.

2.2. Konfiguration der Firmware

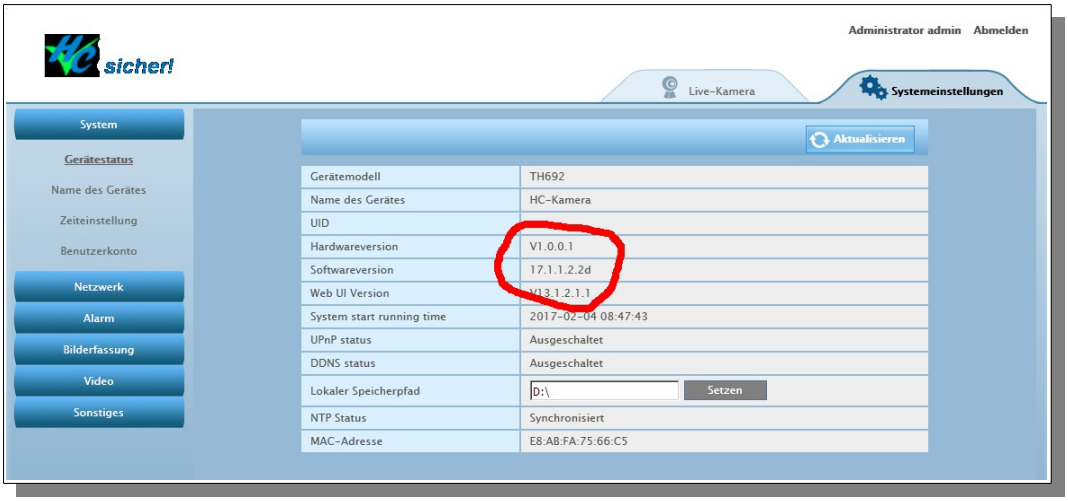
Dieser Abschnitt ist für die originale Firmware und die modifizierte im Wesentlichen gleich. Abweichungen gibt es nur bei der Softwareversion und dem Logo.

Achtung Hinweis:

Das Importieren eines Backups von der alten Firmware sollte unbedingt vermieden werden! Es funktioniert zwar, wäre auch sehr bequem, aber im Hintergrund kommen die mühsam gelöschten Adressen wieder ins System!!

Es werden jetzt nacheinander alle Punkte System, Netzwerk, Alarm und Bilderfassung bearbeitet. Nach jeder Änderung ist auf der gleichen Seite der Button „sichern“ zu betätigen, da ansonsten die Änderungen nach einem Seitenwechsel wieder verloren gehen würden. Zudem sieht man auch an der Meldung „Sichern erfolgreich“ das Abspeichern im den gewünschten Parametern korrekt war. Andernfalls gibt es einen roten Text „Sichern nicht möglich!“.

- Gerätestatus:



- Zeiteinstellung:

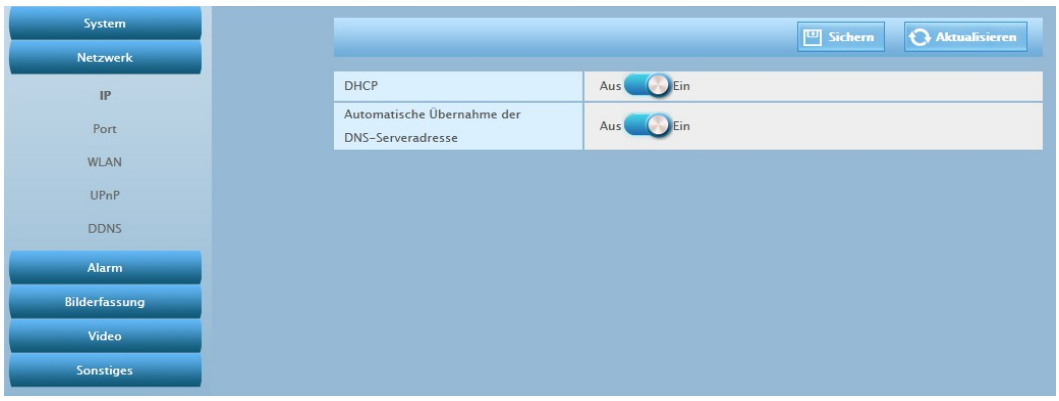


- Benutzerkonto:

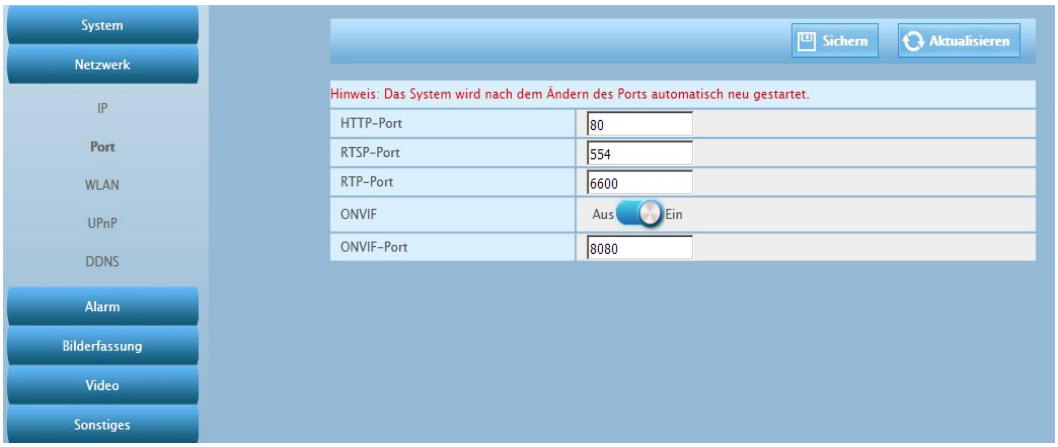
  Die Kamera unterstützt einen 2-Level Zugriff. Nur der Admin kommt an die Einstellungen heran. Die Verwendung des Accounts „guest“ ist deshalb nicht notwendig, es reicht die Passwörter dafür zu löschen, die anderen zu ändern und zu „Sichern“.



- IP



- Port



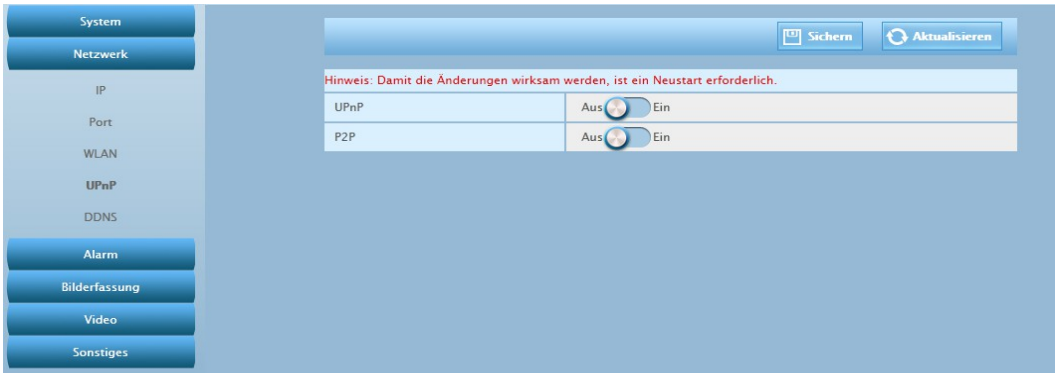
- WLAN

  Wenn schon WLAN, dann ist auch zwingend auf Verschlüsselung zu achten!

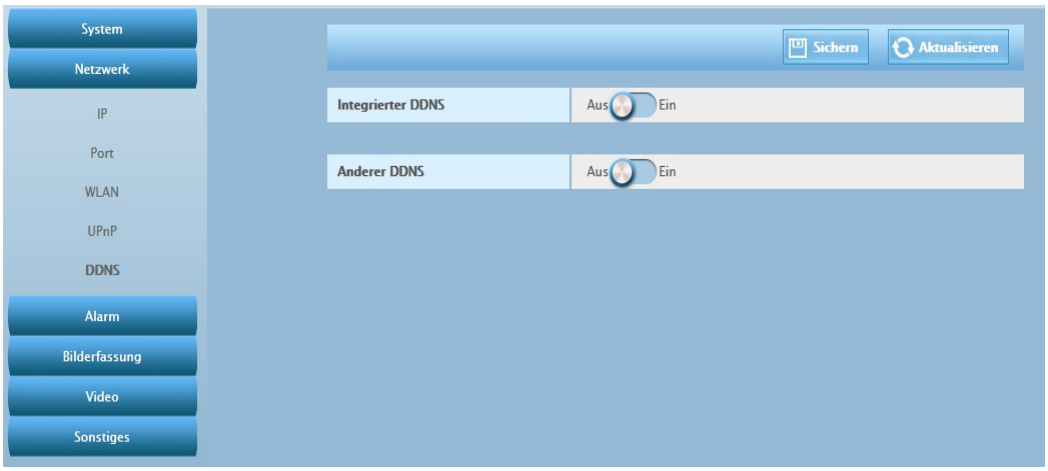


Nach dem WLAN-Test wird mit „OK“ abgespeichert:

- UpnP

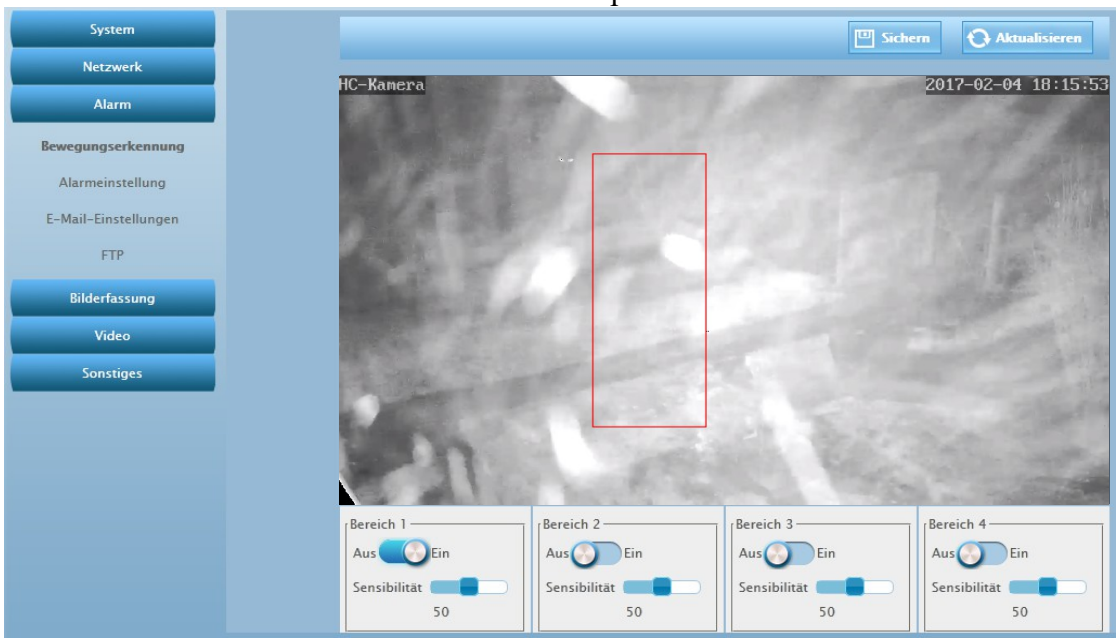


- DDNS



- Bewegungserkennung

  Hier kann man bis zu 4 Bereiche inklusive Empfindlichkeit einstellen.

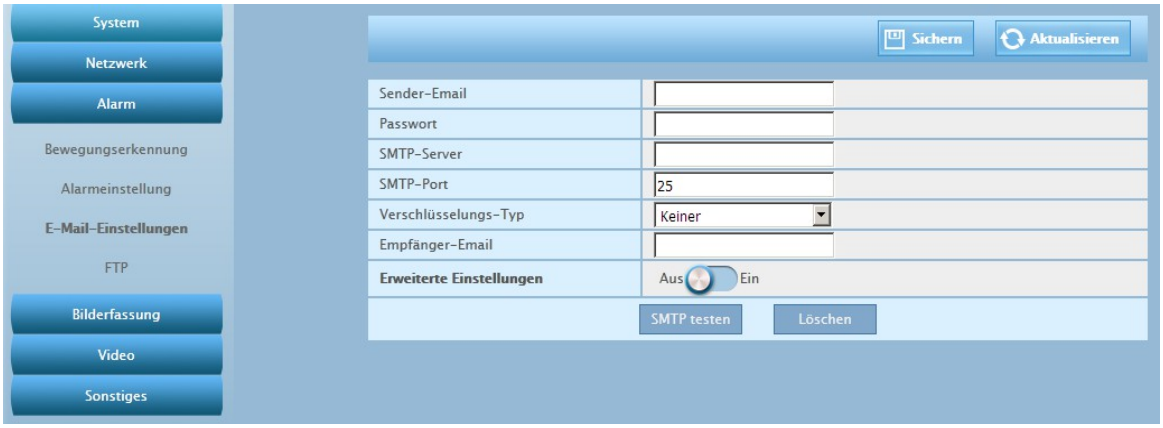


- Alarmeinstellung

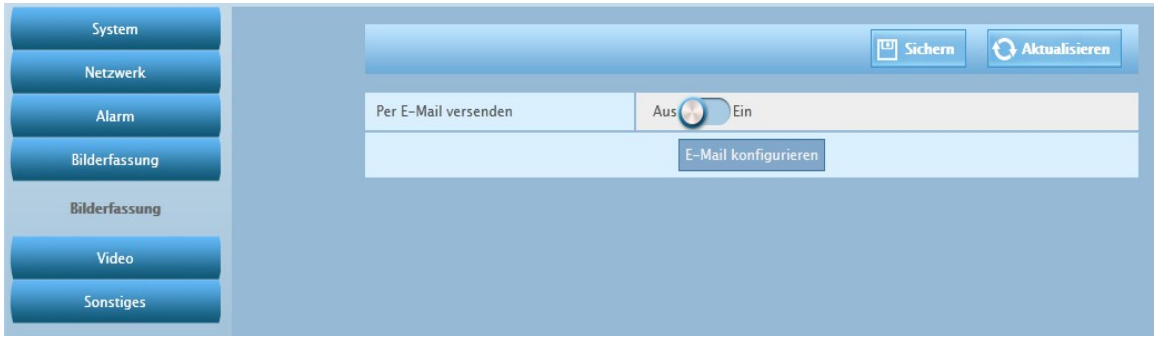
  Im Alarm-Auslösezeitplan kann man durch Klicken in das entsprechende Feld die Auslösung zu bestimmten Zeiten abschalten.



- E-Mail-Einstellungen

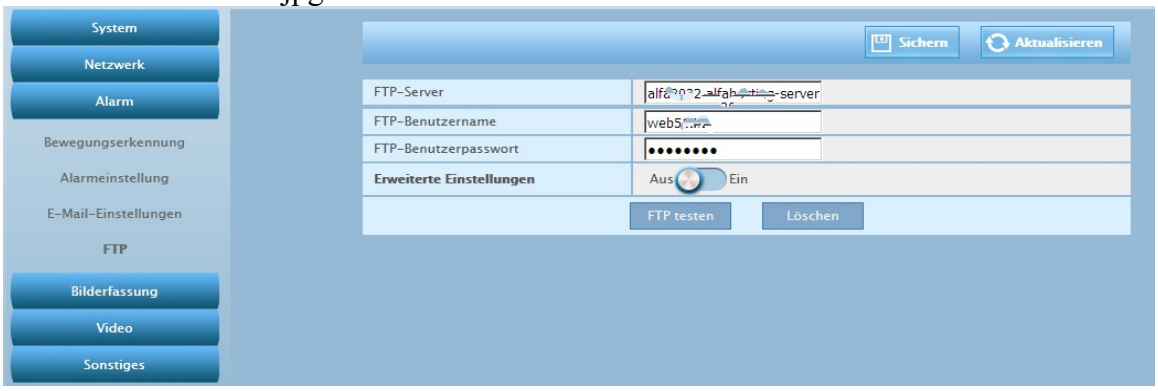


und ...



- FTP

  Nach erfolgreichem Test der Verbindung findet man eine Datei in der Form T17020311540500.jpg auf dem FTP-Server.



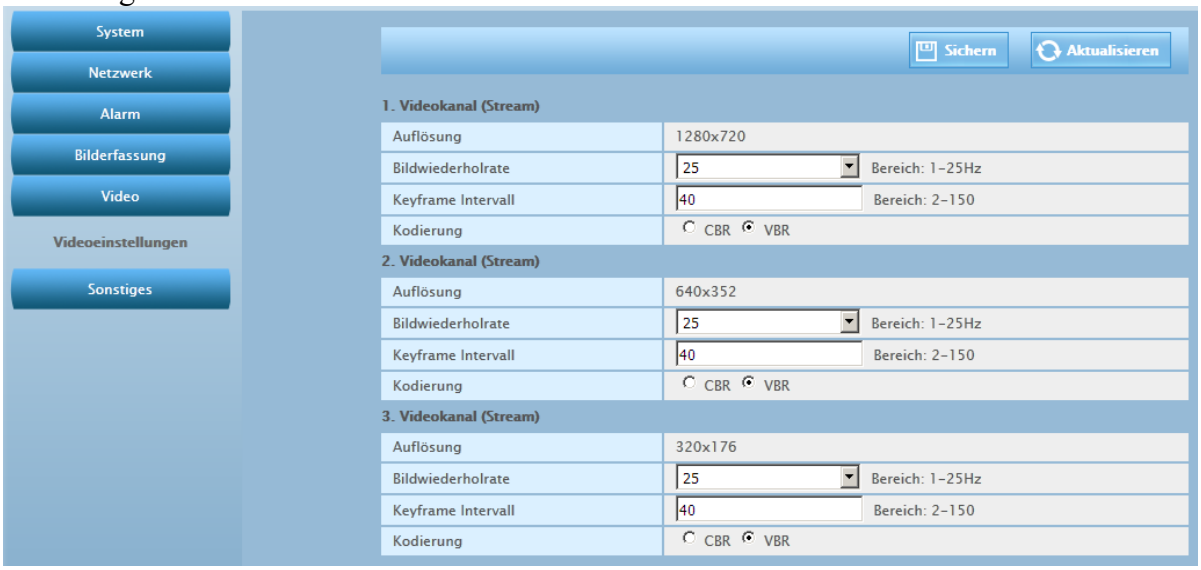
  Für den Hauscomputer sind es folgende Einstellungen:



  Der Pfad bei HC_V2 heißt: /flash/stick/ipkamera/

- Videoeinstellungen

  Hier gibt es nichts weiter zu tun..

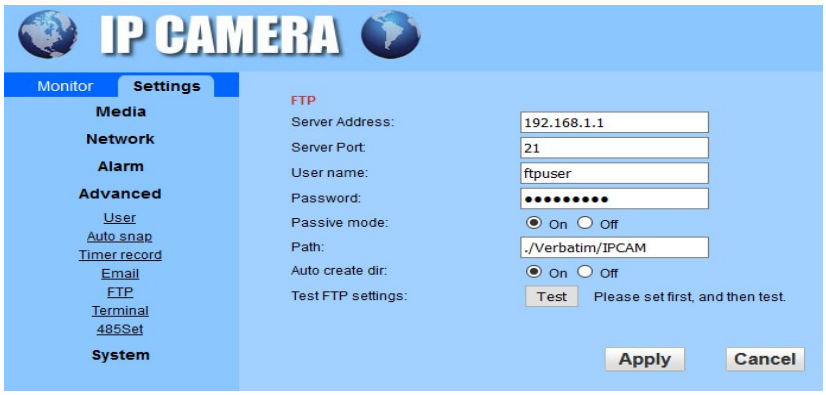


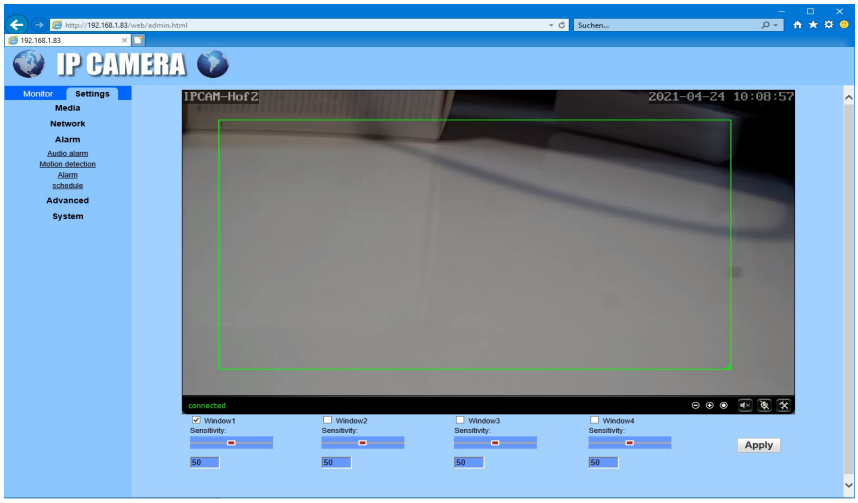
Wenn man alles eingestellt und getestet hat, kann über „Sonstiges“ ein Backup mit allen Einstellungen machen.

3. Sicherung von Kameras ohne Modifizierung der Firmware

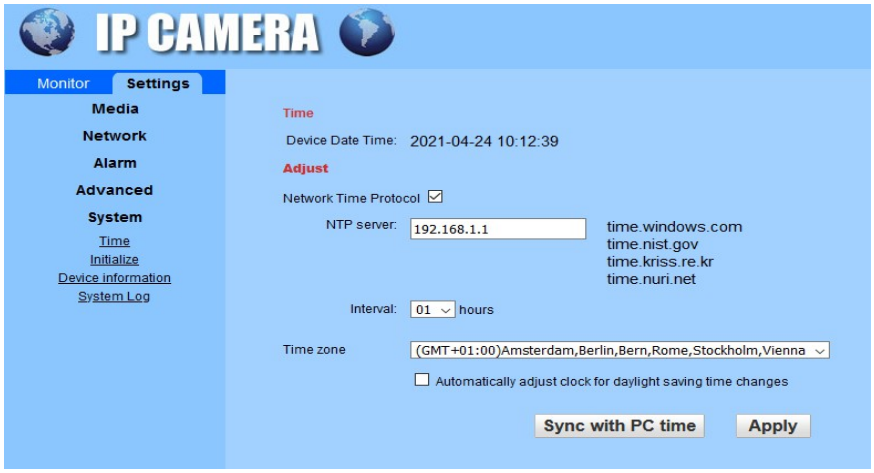
Soll eine Kamera in einem Subnetz integriert werden, deren Firmware weder überprüft, noch geändert werden kann, so gibt es nur einen Weg den Abfluss sensibler Subnetz-Daten (Kennung/Passwörter) bzw. die Übernahme der Kamera durch Fremde zu verhindern: Die Kamera darf niemals Verbindung zum Internet erhalten. Dann empfiehlt sich folgende Herangehensweise:

- Kamera für Einstellungszwecke zunächst mit einem Laptop/PC direkt verbinden, d.h. ohne Zugriff der Kamera auf das Internet
- In den Einstellungen der Kamera folgende Parameter festlegen:
  - eine feste IP-Adresse für die spätere Nutzung vergeben
  - Nutzerkennungen/Passwörter der Kamera individualisieren
  - Bewegungserkennung und Alarmreaktionen (Speicherung von Bildern/Video lokal auf Karte oder per FTP) einstellen (eventuell ist dazu der alte Internet-Explorer unter Windows erforderlich)





- Als Zeitserver den Router festlegen



- Im Router des Subnetzes die MAC-Adresse der Kamera und die IP-Adresse anmelden und im Profil für die Kamera den Zugriff auf das Internet untersagen (z.B. einheitliches Profil „nur_intern“ einrichten)
- Den Router als Zeitserver konfigurieren
- Die Kamera vom Laptop/PC trennen und direkt mit dem Subnetz verbinden (LAN/WLAN)
- In den Einstellungen der Kamera die Alarmauslösungen testen und kontrollieren
- Alle Einstellungen notieren
- Fertig!