

7links™



**FERNSTEUERBARE INDOOR-
WLAN-IP-KAMERA**
mit SD-Speicher & Infrarot

Deutsch

Bedienungsanleitung

PX-3677-675



**FERNSTEUERBARE INDOOR-
WLAN-IP-KAMERA**
mit SD-Speicher & Infrarot

INHALTSVERZEICHNIS

EINLEITUNG

Ihre neue IP-Kamera	6
Verwendung dieser Bedienungsanleitung	7
Wichtige Hinweise zu Beginn	9
Sicherheit & Gewährleistung	9
Informationen zur Entsorgung von elektrischen und elektronischen Geräten	10
Konformitätserklärung	10
Produktinformationen	11
Lieferumfang	11
Technische Daten	12
Systemvoraussetzungen	12
Detailsansicht	14

INSTALLATIONSANLEITUNG

Installation	16
Produktempfehlungen	16
Vorbereitung	17
Anschluss und Inbetriebnahme	18
Browser-Zugriff auf die Kamera	24
ActiveX – Steuerelemente aktivieren	26
Sicherheitseinstellungen deaktivieren	26
OCX installieren	33
Sicherheitseinstellungen wiederherstellen	34
WLAN-Einstellungen	37
Verbindung einrichten	38
WEP	41
Verbinden	42
Montage	43

VERWENDUNG

Grundlegende Steuerung	44
Passwort einstellen	45
Benutzerkonten einrichten	47
WLAN-Einstellungen	49
Mehrere Kameras im Netzwerk verbinden	51
Updates installieren	54
Videoaufnahmen	58
Kurs festlegen	60

ANHANG

Anschluss von Bewegungsmeldern	61
Einstellungen des Alarmdienstes	61
I/O Pins	62
I/O Verbindung bei Alarm	63
Lösung häufiger Probleme (Troubleshooting)	64
Die Kamera wird im Netzwerk nicht erkannt	64
Das Passwort und/oder der Benutzername sind verloren gegangen	64
Die Bilderübertragungsrate ruckelt und/oder ist von minderer Qualität	65
Basiswissen Netzwerke	66
Hardware	66
Grundlegende Netzwerkbegriffe	67
Dienste in Netzwerken	72
Sicherheitsmaßnahmen in WLAN-Netzwerken	76
Checkliste für die Konfiguration	78



EINLEITUNG

IHRE NEUE IP-KAMERA





Sehr geehrte Kunden,

vielen Dank für den Kauf dieser Wireless-Netzwerk-IP-Kamera, einer leistungsstarken kabellosen Netzwerkkamera für Bilder und Videos mit hoher Qualität und mit Audio vor Ort via Internetverbindung.

Bitte beachten Sie die folgenden Hinweise zum Aufbau der Bedienungsanleitung und lesen Sie alle Kapitel sorgfältig durch, damit Sie Ihre neue Kamera optimal einsetzen können.



VERWENDUNG DIESER BEDIENUNGSANLEITUNG**Verwendete Symbole**

	Dieses Symbol steht für mögliche Gefahren und wichtige Informationen im Umgang mit diesem Produkt. Es wird immer dann verwendet, wenn Sie eindringlich auf etwas hingewiesen werden sollen.
	Dieses Symbol steht für nützliche Hinweise und Informationen, die im Umgang mit dem Produkt helfen sollen „Klippen zu umschiffen“ und „Hürden zu nehmen“.
	Dieses Symbol wird für beispielhafte Anwendungen und Erläuterungen verwendet, die oft komplexe Vorgehensweisen veranschaulichen und begreiflich machen sollen.
	Dieses Symbol wird oftmals hinter Fachbegriffen zu finden sein, zu denen weitere Erläuterungen im Glossar zu finden sind. Das Glossar soll dabei helfen, diese Fachbegriffe für den Laien verständlich zu machen und in einen Zusammenhang zu rücken.

Verwendete Textmittel

GROSSBUCHSTABEN	Großbuchstaben werden immer dann verwendet, wenn es gilt Tasten, Anschluss- oder andere Produkt-Beschriftungen kenntlich zu machen.
Fettschrift	Fettschrift wird immer dann eingesetzt, wenn Menüpunkte oder genau so bezeichnete Ausdrücke in der Software des Produktes verwendet werden.
1. Aufzählungen 2. Aufzählungen 3. Aufzählungen	Aufzählungen werden immer dann verwendet, wenn Sie eine bestimmte Reihenfolge von Schritten befolgen sollen, oder die Merkmale des Produktes beziffert werden sollen.

Gliederung

Diese Anleitung ist in vier grundlegende Bestandteile untergliedert:

Kapitel 1: Einleitung	Erläuterungen zur Nutzung dieser Anleitung, Wichtige Hinweise zur Sicherheit im Umgang mit dem Produkt, Übersicht über das Produkt
Kapitel 2: Installation	Detaillierte Anleitung zur Installation und Inbetriebnahme der IP-Kamera und zur grundlegenden Konfiguration.
Kapitel 3: Verwendung	Hinweise zur Steuerung und den erweiterten Einstellungen der IP-Kamera
Anhang	Troubleshooting (Problemlösungen), Glossar, Konformitätserklärung und Index

WICHTIGE HINWEISE ZU BEGINN

Sicherheit & Gewährleistung

- Diese Bedienungsanleitung dient dazu, Sie mit der Funktionsweise dieses Produktes vertraut zu machen. Bewahren Sie diese Anleitung daher stets gut auf, damit Sie jederzeit darauf zugreifen können.
- Sie erhalten bei Kauf dieses Produktes zwei Jahre Gewährleistung auf Defekt bei sachgemäßem Gebrauch. Bitte beachten Sie auch die allgemeinen Geschäftsbedingungen!
- Bitte verwenden Sie das Produkt nur in seiner bestimmungsgemäßen Art und Weise. Eine anderweitige Verwendung führt eventuell zu Beschädigungen am Produkt oder in der Umgebung des Produktes.
- Ein Umbauen oder Verändern des Produktes beeinträchtigt die Produktsicherheit. Achtung Verletzungsgefahr!
- Öffnen Sie das Produkt niemals eigenmächtig. Führen Sie Reparaturen nie selber aus!
- Behandeln Sie das Produkt sorgfältig. Es kann durch Stöße, Schläge oder Fall aus bereits geringer Höhe beschädigt werden.
- Halten Sie das Produkt fern von Feuchtigkeit und extremer Hitze.
- Tauchen Sie das Produkt niemals in Wasser oder andere Flüssigkeiten.



ACHTUNG

Es wird keine Haftung für Folgeschäden übernommen. Technische Änderungen und Irrtümer vorbehalten!

Informationen zur Entsorgung von elektrischen und elektronischen Geräten

Ihr neues Produkt wurde mit größter Sorgfalt entwickelt und aus hochwertigen Komponenten gefertigt. Trotzdem muss das Produkt eines Tages entsorgt werden. Die durchgestrichene Mülltonne bedeutet, dass Ihr Produkt am Ende seiner Lebensdauer getrennt vom Hausmüll entsorgt werden muss. Bitte bringen Sie in Zukunft alle elektrischen oder elektronischen Geräte zu den eingerichteten kommunalen Sammelstellen in Ihrer Gemeinde. Diese nehmen Ihre Geräte entgegen und sorgen für eine ordnungsgemäße und umweltgerechte Verarbeitung. Dadurch verhindern Sie mögliche schädliche Auswirkungen auf Mensch und Umwelt, die sich durch unsachgemäße Handhabung von Produkten am Ende von deren Lebensdauer ergeben können. Genaue Informationen zur nächstgelegenen Sammelstelle erhalten Sie bei Ihrer Gemeinde.

Konformitätserklärung

Hiermit erklärt Pearl Agency, dass sich dieses Produkt PX-3677 in Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie 1999/5/EG befindet.

Pearl Agency
Pearl-Str. 1-3
79426 Buggingen
Deutschland
22.03.2012

Kucharski

Die ausführliche Konformitätserklärung finden Sie unter www.pearl.de. Klicken Sie auf der linken Seite auf den Link **Support (FAQ, Treiber & Co.)**. Geben Sie anschließend im Suchfeld die Artikelnummer PX-3677 ein.

Importiert von:
PEARL Agency GmbH
PEARL-Straße 1-3
D-79426 Buggingen



PRODUKTINFORMATIONEN

Die IP-Kamera bietet sowohl dem Heimanwender als auch professionellen Nutzern eine Vielzahl an Anwendungsgebieten. Für optimalen Schutz stehen außerdem die zum heutigen Sicherheitsstandard gehörenden Verschlüsselungsvarianten WPA und WPA2 zur Verfügung. Mit den 802.11b/g Standards erreichen Sie Datendurchsatzraten bis zu 54 MBit/s. Die externe Antenne ermöglicht hierbei einen verlustarmen Datentransfer über weite Strecken. Unter normalen Umweltbedingungen kann die Kamera im gesamten Sendegebiet Ihres WLAN-Routers arbeiten. Für die Fernüberwachung kann die Kamera Momentaufnahmen und Videos als Emails versenden oder diese sogar auf voreingestellte FTP-Server laden.

Lieferumfang

- IP-Kamera
- WLAN-Antenne
- Netzkabel (RJ45)
- Wandhalterung
- GPIO-Stecker
- Netzteil
- Software-CD
- Bedienungsanleitung



HINWEIS:

Für den Betrieb benötigen Sie zusätzlich eine microSD-Karte.

Technische Daten

- 1/4"-CMOS-Sensor (Farbe)
- Auflösung: 640 x 480 Pixel (VGA) / 320 x 240 Pixel (QVGA)
- Nachtsicht durch 10 IR-LEDs: bis 10 m Reichweite
- Lichtempfindlichkeit: 0,5 Lux
- Sichtfeld: horizontal 270°, vertikal 120°
- Bildfrequenzrate: max. 30 fps
- Bewegungserkennung mit automatischem Bild-Versand per E-Mail
- Integriertes Mikrofon
- Unterstützt die wichtigsten Internet- und Einwahlprotokolle: HTTP, FTP, TCP/IP, SMTP, DHCP, UDP, UPnP, DDNS, PPPoE
- WLAN: Übertragungsgeschwindigkeit bis 54 Mbit/s (IEEE 802.11g) mit WEP-Verschlüsselung
- Integrierter Web-Server
- Maße: 100 mm x 125 mm
- Stromversorgung: 5 V / 2 A

Systemvoraussetzungen


- **Netzwerk**
 - LAN: 10 Base-T Ethernet oder 100 Base-TX Fast Ethernet
 - WLAN: IEEE 802.11b/g.
- **Computer für Webbrowser-Zugriff**
 - Betriebssystem: Microsoft Windows 2000/XP/Vista/7
 - Arbeitsspeicher: 128 MB RAM
 - Auflösung: 800 x 600 oder besser
 - Browser: Microsoft Internet Explorer (6.0 oder neuer)
 - Prozessor: Intel Pentium III 800 MHz oder besser

Angeschlossene Kameras	Prozessor	Arbeitsspeicher
1	Pentium III / 800 MHz	512 MB RAM
2 bis 4	Pentium 4 / 1,3 GHz	512 MB RAM
5 bis 9	Pentium 4 / 2,4 GHz	1 GB RAM

Statt eines Intel-Pentium-Prozessors kann jeweils auch ein AMD-Prozessor mit vergleichbaren Leistungswerten verwendet werden. Die hier angegebenen Daten sind die minimal benötigten Werte. Höhere Leistungswerte erleichtern in jedem Fall die Bedienung und beschleunigen die Installation und Verwendung.



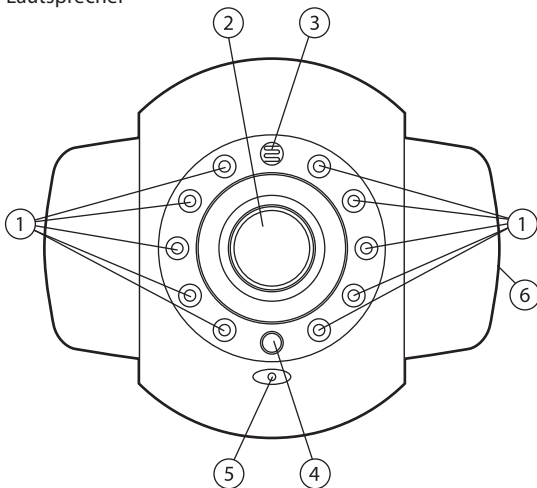
HINWEIS:

*Die Software der Kamera verwendet ActiveX-
Steuerelemente, verwenden Sie daher nur den Internet
Explorer und keine anderen Browser  wie Mozilla
Firefox, Apple Safari oder Google Chrome.*

DETAILSANSICHT

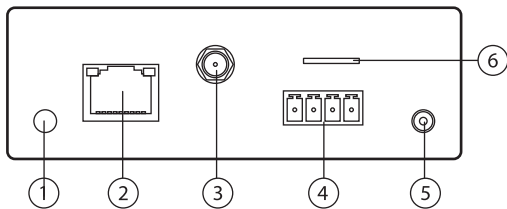
Vorderseite

1. Infrarot-LEDs
2. Linse (CMOS-Sensor mit fest integrierter Linse)
3. Lichtsensor
4. Netzwerk-LED
5. Mikrofon
6. Lautsprecher



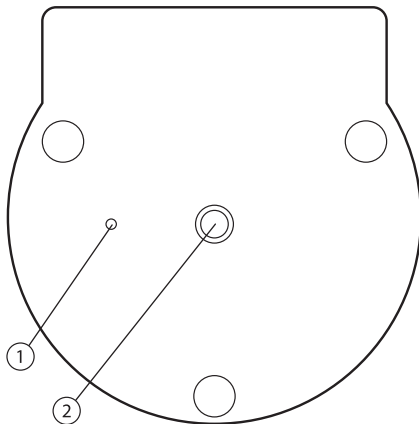
Rückseite

1. Kopfhörerausgang
2. RJ45 Ethernet-Anschluss
3. Antenne
4. I/O Alarm-Anschlüsse
5. Netzteil-Anschluss
6. microSD-Slot



Unterseite

1. Reset-Taste
2. Halterungsöffnung



INSTALLATIONSANLEITUNG

INSTALLATION



ACHTUNG:

Nehmen Sie die Kamera in Betrieb und versichern Sie sich, dass sowohl die LAN- als auch die WLAN-Funktion problemlos funktionieren, bevor Sie die Kamera fest montieren. Weitere Hinweise zur Montage finden Sie am Ende dieses Kapitels.



HINWEIS:

Viele der Fachbegriffe werden im Anhang „Basiswissen Netzwerke“ erläutert (S. 78). Sollten dennoch Fragen bezüglich der Installation bestehen, können Sie sich gerne an die Service-Hotline Ihres Fachhändlers wenden.

Produktempfehlungen

Zusätzlich zu den unbedingt notwendigen Zubehörteilen empfehlen wir Ihnen für die Erweiterung Ihres Netzwerkes und die Verwendung der Kamera folgende Artikel, die Sie unter www.pearl.de bestellen können:

PE-5586-675	ConneTec 10/100MBit Netzwerk-Switch 5-Port USB mit blauen LEDs
PX-6516-675	TP-LINK 54Mbit WLAN-USB-Dongle „TL-WN321G“ USB2.0 (802.11g/b)
PE-4454-675	revolt Profi-Steckdosenleiste mit Netzwerkschutz




Vorbereitung







HINWEIS:

Sollten Sie sich bei den folgenden Fragen nicht sicher sein, wird empfohlen, sich an einen Fachmann zu wenden. Eine Fehlkonfiguration der Kamera kann den Zugriff auf diese unmöglich machen.

Für eine reibungslose Installation der Kamera sollten Sie folgende Daten im Vorfeld recherchieren und bereithalten:

- Die Zugangsdaten Ihres Serviceproviders (Internet-Anbieters)
- Die IP-Adresse  des Gateway-Routers .
- Die Art des verwendeten Netzwerks (Infrastructure oder Adhoc).
- Wird in Ihrem Netzwerk bereits ein DHCP-Server  verwendet? Wenn ja – welche Adressräume deckt dieser ab?

Ferner sollten Sie folgendes im Vorfeld beachten:

- Bei der Erstinstallation muss die Kamera direkt über Kabel mit einem Router verbunden werden.
- Beseitigen Sie eventuelle Störquellen im Funktionsbereich Ihres WLAN-Routers. Hierzu gehören Funktelefone, Funküberwachungskameras und andere Geräte, die mit dem 2,4 GHz Band funktionieren.
- Verwenden Sie zwischen Kamera und Router kein Kabel, das länger als 25 m ist – bei ungünstigen Verhältnissen kann es sonst zu einem Spannungsabfall kommen und die Kamera kann keine Signale mehr übertragen.
- Schalten Sie zur Einbindung der Kamera in ein bestehendes Netzwerk alle Firewalls , Virens Scanner, MAC-Adressenfilter  und Verschlüsselungen  Ihres Routers aus.
- Notieren Sie sich die SSID  Ihres bestehenden WLAN-Netzwerks.





HINWEIS:

Im Anhang dieser Anleitung finden Sie eine Checkliste zur Installation und Inbetriebnahme. Trennen Sie die Liste mit einer Schere heraus und verwenden Sie sie, um die einzelnen Punkte abzuarbeiten.

Anschluss und Inbetriebnahme

**ACHTUNG:**

Beachten Sie unbedingt die Reihenfolge der nächsten Schritte und führen Sie sie genau so aus.

1. Verwenden Sie das Netzkabel, um die Kamera mit einem freien Ethernet-Anschluss Ihres Routers  oder einem Netzwerkschwitch , der an diesen angeschlossen ist, zu verbinden. Verbinden Sie dann das Netzteil mit der Stromversorgung und dem Stromanschluss der IP-Kamera-Kabelverbindung.

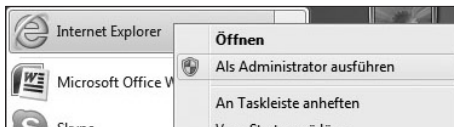
**HINWEIS:**

Es wird empfohlen, das Netzteil nur mit einer Mehrfachsteckdosenleiste mit integriertem Überspannungsschutz zu verbinden.

2. Starten Sie Ihren Computer und führen Sie die Softwareinstallation aus, um auf die Kamera zuzugreifen.
3. Legen Sie die mitgelieferte Software-CD in ein freies CD-/DVD-Laufwerk Ihres Computers.

**ACHTUNG:**

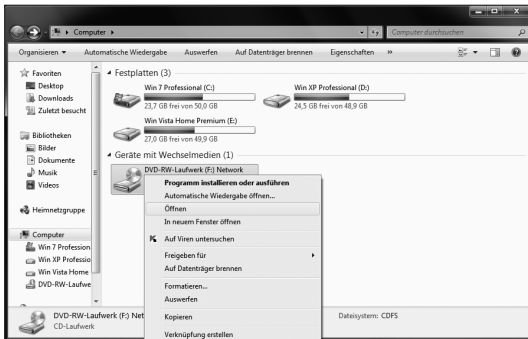
Für die Verwendung mit der Kamera müssen Sie ihren Browser grundsätzlich als Administrator ausführen.



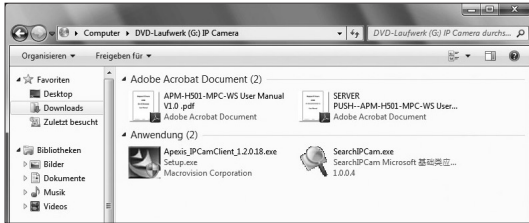
4. Wählen Sie **autorun.exe ausführen**, nachdem Windows die CD erkannt hat. Fahren Sie dann mit Schritt 5 fort.



Sollte die CD nicht automatisch erkannt werden, öffnen Sie Ihren **Arbeitsplatz/Computer** und wählen Sie das Laufwerk mit einem Rechtsklick aus.



Wählen Sie **Explorer/Öffnen**, um den Inhalt der CD anzeigen zu lassen.



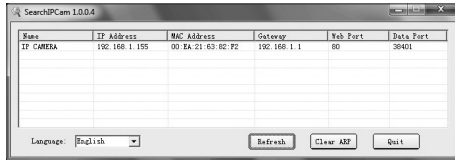
5. Starten Sie die Datei **SearchIPCam** mit einem Doppelklick.



HINWEIS:

IP-Finder anderer Kameras funktionieren hier nicht.

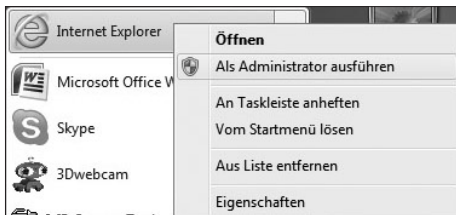
Im Fenster „SearchIPCam“ werden Ihnen angeschlossene Kameras sowie deren IP und MAC Adressen angezeigt.



ACHTUNG:

Geben Sie die Adresse als Vertrauenswürdige Seite in den Browser ein.

Starten Sie Ihren Internet Explorer als Administrator.



HINWEIS:

Wenn Sie den Microsoft Internet Explorer verwenden, müssen im nächsten Abschnitt Active-X Steuerelemente installiert werden. Beachten Sie hierzu die Hinweise im nächsten Abschnitt. Andere Browser wie z.B. Mozilla Firefox können die benötigten ActiveX Steuerlemente nicht darstellen und zeigen nur ein begrenztes Funktionsmenü der Kamera an. Beachten Sie hierzu auch den Abschnitt „Andere Browser verwenden“.

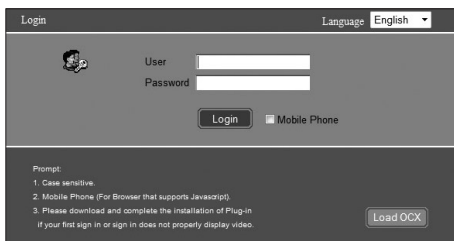
Geben Sie die angezeigte IP-Adresse in die Adresszeile Ihres Browsers ein.



BEISPIEL:

Wenn die Kamera unter der IP-Adresse „168.198.0.10“ angezeigt wurde muss die Eingabe im Internet Explorer „http:// 168.198.0.10“ lauten.

Im nächsten Fenster werden Sie nach dem Passwort gefragt. Geben Sie in beide Zeilen **admin** ein. Klicken Sie auf **OK**.



Language English

User

Password

Login Mobile Phone



Prompt:

1. Case sensitive
2. Mobile Phone (For Browser that supports Javascript)
3. Please download and complete the installation of Plug-in if your first sign in or sign in does not properly display video.

Load OCX

**HINWEIS:**

Wählen Sie **Language** und klicken Sie auf **Deutsch**.

Im Browser  erscheint jetzt die Online-Steuerung der IP-Kamera. Die Kamera kann nun von jedem Computer, der mit Ihrem Netzwerk verbunden ist, angesteuert und über den Browser  bedient werden.



Beachten Sie die Hinweise im folgenden Abschnitt, um auf die Kamera zuzugreifen. Danach können Sie die WLAN-Einstellungen vornehmen und die grundlegenden Funktionen testen.

Klicken Sie auf **ActiveX laden**.

Bitte beachten Sie:
1. Sie haben keine ActiveX Steuerelemente installiert.
2. Die vorhandenen ActiveX Steuerelemente sind veraltet.

Klick **ActiveX laden** ActiveX installieren, Aktualisieren Sie den Browser, um das Video zu starten.

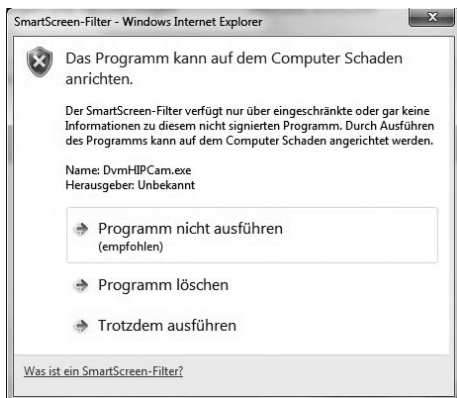
Klicken Sie auf **Ausführen**.



Klicken Sie auf **Aktionen**.



Klicken Sie dann auf **Trotzdem ausführen**.



Klicken Sie nach der Installation auf **Schließen** und aktualisieren Sie die Seite anschließend.

Loggen Sie sich nun erneut ein.

BROWSER-ZUGRIFF AUF DIE KAMERA

Sie können die folgenden Browser verwenden, um auf die Kamera zuzugreifen.

Anbieter	Browser
Microsoft	Internet Explorer
Google	Chrome
Mozilla	Firefox
Macintosh	Safari

Auf dem Startbildschirm der Kamera können Sie auswählen, ob Sie den Internet Explorer oder einen anderen Browser verwenden wollen (Server Push Modus).



Login

Language English

User

Password

Mode Server Push

Login Mobile Phone

Prompt:

1. Case sensitive.
2. Mobile Phone (For Browser that supports Javascript).
3. Please download and complete the installation of Plug-in

if your first sign in or sign in does not properly display video.

Klicken Sie dann auf **Anmelden** unter **ActiveX Modus** oder **Server Push Modus**, je nachdem ob Sie den Internet Explorer oder einen anderen Browser verwenden.



ACHTUNG:

*Im **Server Push Modus** sind nicht alle Funktionen der IP-Kamera verfügbar.*



HINWEIS:

*Für die Verwendung des Microsoft Internet Explorers ist es notwendig, weitere Einstellungen vorzunehmen. Beachten Sie hierzu den nächsten Abschnitt. Wenn Sie einen anderen Browser verwenden und **Server Push Modus** gewählt haben, überspringen Sie den nächsten Abschnitt und fahren Sie mit „WLAN-Einstellungen“ fort.*



ACTIVEX – STEUERELEMENTE AKTIVIEREN

Falls Sie den Microsoft Internet Explorer verwenden und den **ActiveX Modus** ausgewählt haben, müssen vor der weiteren Verwendung einige Einstellungen vorgenommen werden.



HINWEIS:

Die exakte Anzeige hängt von der von Ihnen verwendeten Version des Microsoft Internet Explorers ab.

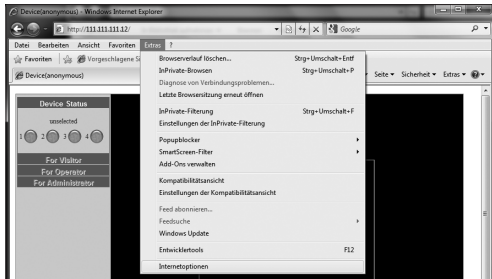
Sicherheitseinstellungen deaktivieren



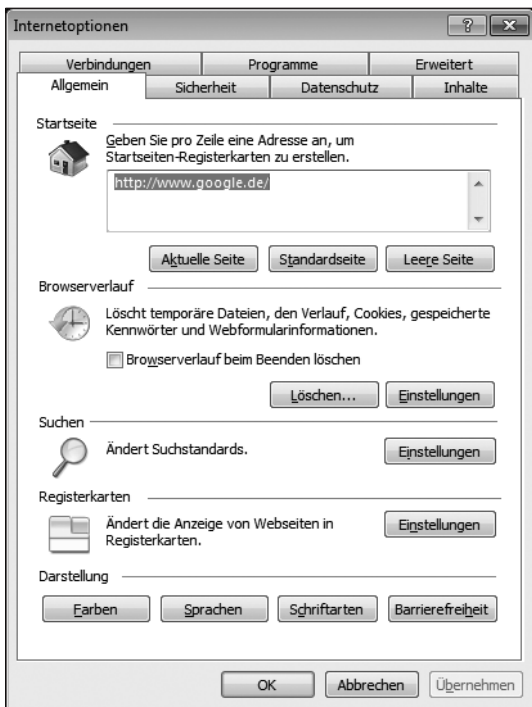
HINWEIS:

Für die Verwendung der Kamera müssen ActiveX-Steuerelemente auf Ihrem Computer installiert werden. Dies kann nur durchgeführt werden, wenn für die Dauer der Installation die Sicherheitseinstellungen des Internet Explorers deaktiviert werden. Die Sicherheitseinstellungen werden im letzten Abschnitt dieses Kapitels wiederhergestellt, damit Ihr System nicht gefährdet wird.

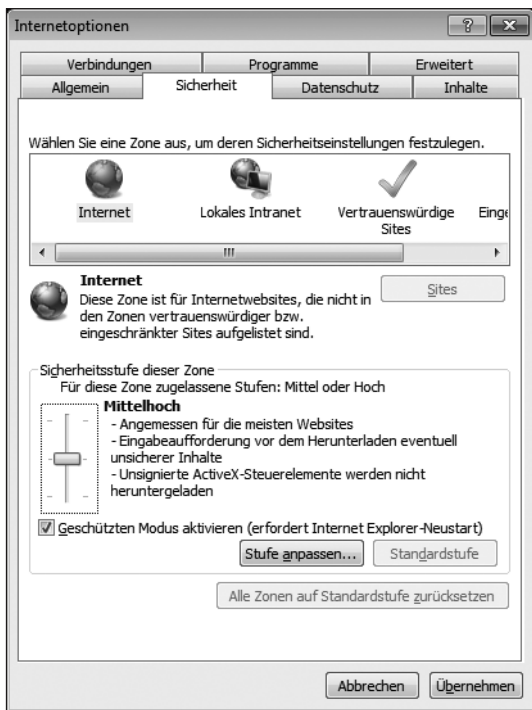
Öffnen Sie das Menü **Extras** Ihres Internet Explorers und wählen Sie den Menüpunkt **Internetoptionen**.



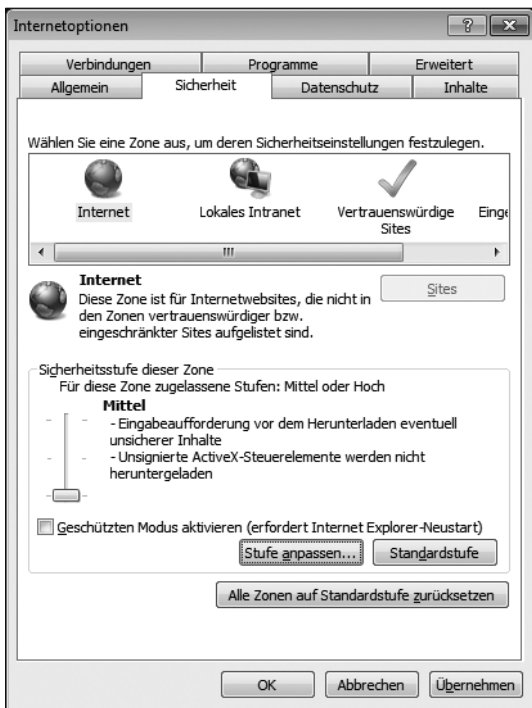
Es erscheinen die allgemeinen Internetoptionen. Klicken Sie auf **Sicherheit**.



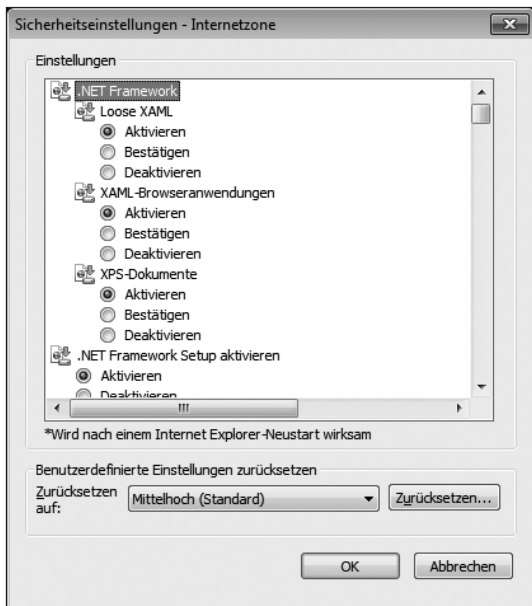
Fahren Sie mit der Maus in den Bereich **Sicherheitsstufe dieser Zone**. Die Sicherheitseinstellungen sind normalerweise auf **Mittelhoch** oder **Hoch**.



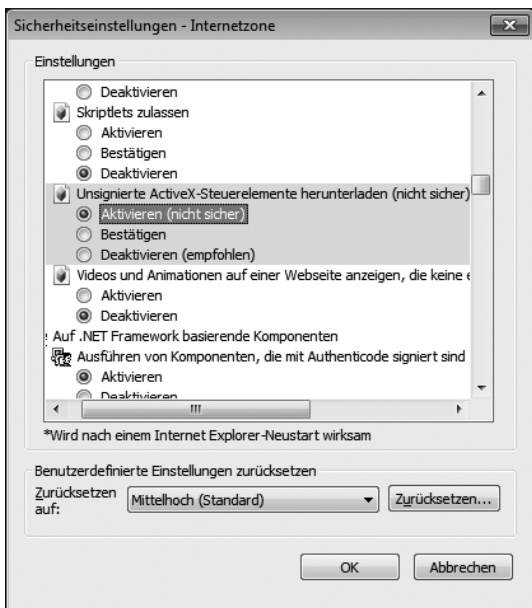
Ziehen Sie den Regler mit der Maus ganz nach unten auf **Mittel** und entfernen Sie den Haken bei **Geschützten Modus aktivieren**.



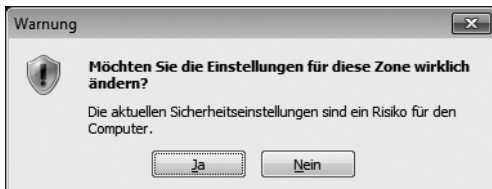
Klicken Sie auf **Stufe anpassen...**, um das Fenster **Sicherheitseinstellungen – Internetzone** zu öffnen.



Scrollen Sie nach unten, bis Sie den Punkt **Unsignierte ActiveX-Steuerlemente herunterladen** finden. Wählen Sie **Aktivieren (nicht sicher)** und klicken Sie auf **OK**.



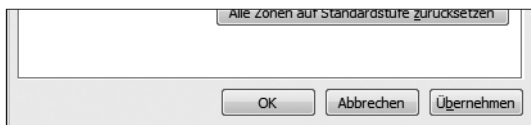
Windows verlangt eine Bestätigung, um die Sicherheitseinstellungen zu ändern. Klicken Sie auf **Ja**, um fortzufahren.



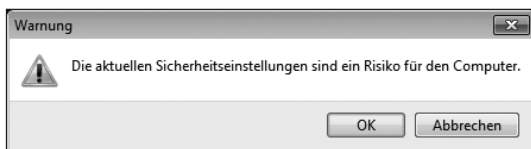
**HINWEIS:**

Windows zeigt Ihnen nun eine Meldung über die geänderten Einstellungen. In der Taskleiste erscheint ein neues Symbol, über das Sie die Einstellungen später wieder bequem zurücksetzen können. Weitere Informationen hierzu erhalten Sie im Abschnitt „Sicherheitseinstellungen wiederherstellen“ (S. 34).

Klicken Sie auf **Übernehmen**.



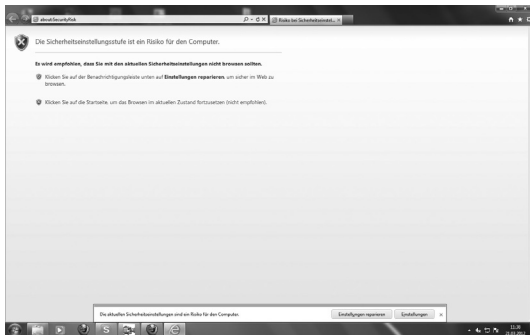
Diese Sicherheitseinstellungen werden von Windows nicht empfohlen und es erscheint eine entsprechende Warnmeldung. Klicken Sie **OK**, um fortzufahren.



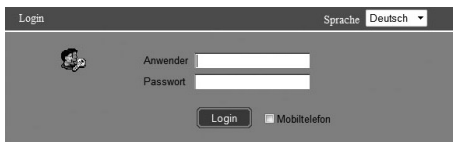
Die benötigten Steuerelemente können jetzt installiert werden und Sie können auf die Kamera zugreifen.

OCX installieren

Vor der Verwendung der Kamera müssen die OCX-Dateien installiert werden. Führen Sie diese Installation aus bevor Sie die Sicherheitseinstellungen Ihres Internet Explorers wie auf Seite 34 beschrieben wiederherstellen.



Wählen Sie die Option **OCX laden** nachdem Sie die Kamera aufgerufen haben.



Laden Sie die Datei **DvmHTPCam** aus dem Browser.



Führen Sie die Datei aus und folgen Sie den Anweisungen des Installationsassistenten. Starten Sie Ihren Browser danach neu.

**HINWEIS:**

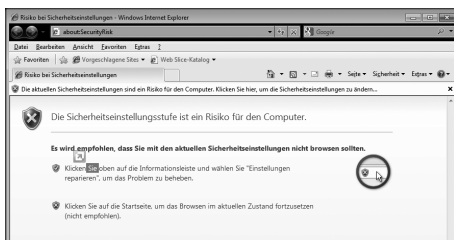
Der Internet Explorer erkennt da Datei als eine Sicherheitsbedrohung und zeigt entsprechende Warnmeldungen ab. Die Kamera kann nur verwendet werden, wenn die Datei trotzdem ausgeführt wird.

Sicherheitseinstellungen wiederherstellen

**ACHTUNG:**

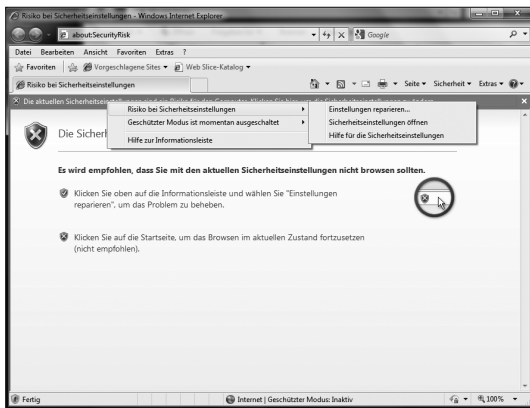
Nach Abschluss der Installation sollten Sie unbedingt die Sicherheitseinstellungen des Microsoft Internet Explorers wiederherstellen, um Ihr System zu schützen.

Beim nächsten Start des Internet Explorers warnt Sie dieser, das die Sicherheitseinstellungen nicht ausreichend sind.

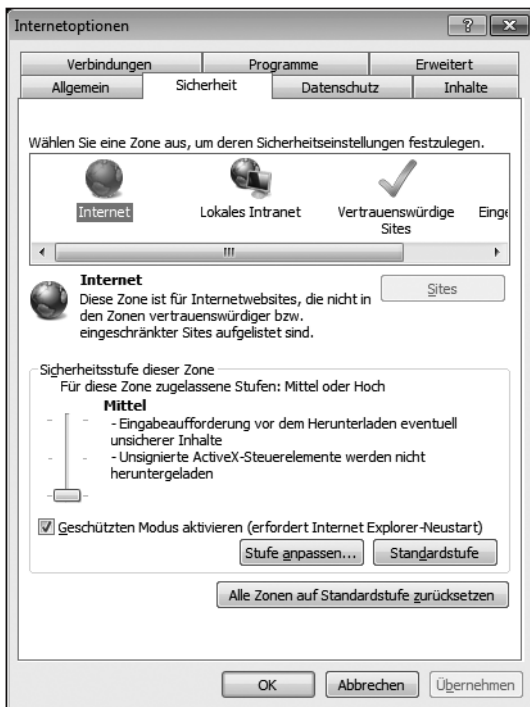


Folgen Sie den Anweisungen des Explorers hinter dem grünen Schild um die Sicherheitseinstellungen wiederherzustellen.

Klicken Sie auf die Anzeige oben im Browserfenster und wählen Sie die Reiter **Risiko bei Sicherheitseinstellungen** und **Sicherheitseinstellungen** öffnen.



Wählen Sie im nächsten Fenster **Alle Zonen auf Standardstufe zurücksetzen**.



Klicken Sie auf **Übernehmen**, um den Vorgang abzuschließen. Die Kamera kann jetzt verwendet werden. Fahren Sie mit dem Abschnitt „WLAN-Einstellungen“ (S. 49) fort, wenn Sie die Kamera kabellos verwenden wollen. Gehen Sie direkt zum Abschnitt „Grundlegende Steuerung“ (S. 44), wenn Sie die Kamera an einem Ethernetkabel betreiben wollen.

WLAN-EINSTELLUNGEN

Sie können die Kamera über das Netzwerkkabel betreiben oder mit Ihrem WLAN verbinden. Im folgenden Abschnitt wird die WLAN-Einstellung beschrieben. Wenn Sie die Kamera weiterhin per Kabel betreiben wollen, können Sie diesen Abschnitt überspringen und direkt mit „Montage“ (S. 43) fortfahren.

Damit die Kamera per WLAN betrieben werden kann, müssen zuerst die Zugangsdaten Ihres Netzwerkes eingegeben werden. Die Einstellungen können Sie nur vornehmen, während die Kamera noch per Kabel mit Ihrem Router verbunden ist. Folgen Sie den Schritten im vorherigen Abschnitt „Anschluss und Inbetriebnahme“ und fahren Sie dann mit Punkt 1 dieses Abschnitts fort.



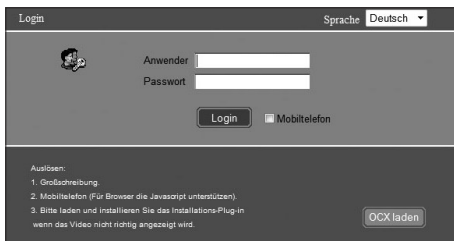
HINWEIS:

Versichern Sie sich, dass Ihr Router keine Whitelist verwendet, da die Kamera sich dann nicht mit dem Netzwerk verbinden kann. Sollte Ihr Netzwerk eine Whitelist verwenden, tragen Sie die IP-Adresse der Kamera in diese ein.

VERBINDUNG EINRICHTEN

Loggen Sie sich wie in den vorherigen Abschnitten beschrieben auf der Startseite der IP-Kamera ein.

Geben Sie als Benutzername und Passwort „Admin“ ein.



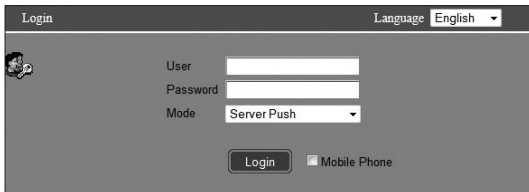
The screenshot shows a login interface with the title "Login" and a language dropdown set to "Deutsch". It features a user icon, input fields for "Anwender" (username) and "Passwort" (password), a "Login" button, and a "Mobiltelefon" checkbox. Below the login fields, there is a section titled "Auslaesen:" with three instructions: 1. Großschreibung, 2. Mobiltelefon (Für Browser die Javascript unterstützen), and 3. Bitte laden und installieren Sie das Installations-Plug-in wenn das Video nicht richtig angezeigt wird. A "OCX laden" button is located at the bottom right.

Wählen Sie als Sprache **Deutsch**



This is a close-up of the language selection dropdown menu, showing "Deutsch" selected.


Klicken Sie auf **Anmelden** unter **Server Push Modus**, wenn Sie einen anderen Browser verwenden .



The screenshot shows the login interface with the title "Login" and a language dropdown set to "English". It features a user icon, input fields for "User" and "Password", a "Mode" dropdown menu set to "Server Push", a "Login" button, and a "Mobile Phone" checkbox.

**ACHTUNG:**

Bei der Verwendung anderer Browser stehen nicht alle Funktionen der IP-Kamera zur Verfügung. Es wird ausdrücklich die Verwendung des Microsoft Internet Explorers empfohlen.

Klicken Sie auf  und wählen Sie **Einstellungen**.

Die Seite für Netzwerkeinstellungen wird nun geladen und das Optionsmenü des Gerätes angezeigt.

Login Sprache **Deutsch** ▼

 Anwender
Passwort


Mobiltelefon

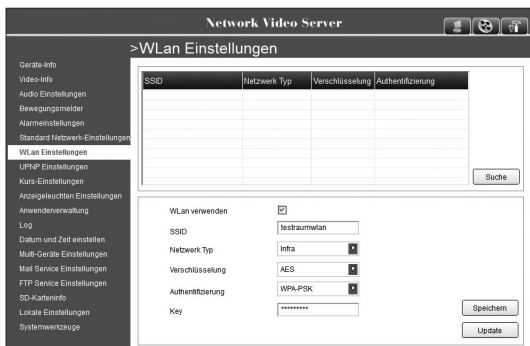
Auslösen:

1. Großschreibung.
2. Mobiltelefon (Für Browser die Javascript unterstützen).
3. Bitte laden und installieren Sie das Installations-Plug-In wenn das Video nicht richtig angezeigt wird.

Setzen Sie einen Haken hinter **WLAN verwenden**, um das erweiterte Menü zu öffnen.

WLAN verwenden

Klicken Sie auf **Suchen**. Die Kamera versucht WLAN-Netzwerke automatisch zu erkennen. Überprüfen Sie, ob Ihr Netzwerk unter **SSID** angezeigt wird. Falls dies nicht der Fall ist, geben Sie Ihre Netzwerk-SSID  manuell ein.



Wählen Sie für Ihren Netzwerktyp **Infra** oder **Adhoc** aus. Für die meisten Heimnetzwerke ist **Adhoc** die richtige Auswahl.



Wählen Sie nun die **Verschlüsselung**, die von Ihrem Netzwerk verwendet wird. Für genauere Informationen hierzu beachten Sie bitte die Hinweise im Handbuch Ihres WLAN-Routers. Falls Sie keine Verschlüsselung verwenden, klicken Sie auf **Speichern** und fahren Sie mit Schritt „Verbinden“ (S.42) fort.




ACHTUNG:

Es wird unbedingt empfohlen Ihr Netzwerk durch eine WPA2-Verschlüsselung zu sichern. Genauere Informationen hierzu finden Sie im Anhang.

Falls Ihr Netzwerk eine WEP-Verschlüsselung verwendet, befolgen Sie die Schritte im folgenden Abschnitt „WEP“ und fahren Sie dann mit „Verbinden“ (S. 42) fort.

Falls Ihr Netzwerk eine WPA- oder WPA2-Verschlüsselung verwendet, befolgen Sie die Schritte im folgenden Abschnitt „WPA und WPA2“ und fahren Sie dann mit „Verbinden“ (S. 53) fort. Klicken Sie auf **Bestätigen**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden“ (S. 53) fort.

WEP

Mit den folgenden Schritten können Sie die IP-Kamera auf ein WEP  geschütztes Netzwerk zugreifen lassen.



The screenshot shows the 'Network Video Server' web interface. The main heading is '> WLAN Einstellungen'. Below this is a table with columns for 'SSID', 'Netzwerk Typ', 'Verschlüsselung', and 'Authentifizierung'. The first row contains 'testraumwlan', 'Intra', 'AES', and 'WPA2-PSK'. Below the table is a search button labeled 'Suche'. Underneath the table, there are several configuration options: 'WLAN verwenden' (checked), 'SSID' (testraumwlan), 'Netzwerk Typ' (Intra), 'Verschlüsselung' (WEP), 'Authentifizierung' (Share Key), 'Key auswählen' (2), and 'Key'. There are 'Speichern' and 'Update' buttons at the bottom right.

SSID	Netzwerk Typ	Verschlüsselung	Authentifizierung
testraumwlan	Intra	AES	WPA2-PSK

WLAN verwenden

SSID

Netzwerk Typ

Verschlüsselung

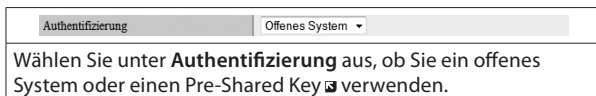
Authentifizierung


Key auswählen

Key


Speichern Update

Wählen Sie zuerst **WEP** aus dem Dropdown-Menü, um die benötigten Eingabefelder zu öffnen.



The image shows a close-up of the 'Authentifizierung' dropdown menu. The selected option is 'Offenes System'. Below the dropdown, there is a text box with the instruction: 'Wählen Sie unter **Authentifizierung** aus, ob Sie ein offenes System oder einen Pre-Shared Key  verwenden.'

Authentifizierung

Wählen Sie unter **Authentifizierung** aus, ob Sie ein offenes System oder einen Pre-Shared Key  verwenden.

Standard TX Schlüssel

1 ▾

Wählen Sie hier den Schlüssel aus, der von Ihrem Netzwerk als Standard verwendet wird.

Geben Sie den Shared Key Ihres Netzwerks ein und geben Sie an, ob dieser eine 64- oder 128-Bit-Verschlüsselung verwendet. Sie müssen nur den Key angeben, dessen Nummer Sie beim vorherigen Punkt angegeben haben.

Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden“ im nächsten Abschnitt fort. Die Kamera startet sich neu, um die neuen Einstellungen zu laden.

Verbinden

Nachdem die Einstellungen der vorherigen Abschnitte vorgenommen wurden, können Sie die IP-Kamera auch kabellos ansteuern. Trennen Sie das Ethernetkabel und schrauben Sie die Antenne hinten an die IP-Kamera. Starten Sie dann Ihren Browser neu und geben Sie die IP-Adresse der Kamera erneut ein. Die Login-Seite der Kamera wird geladen.

Login Sprache Deutsch ▾

Anwender

Passwort

Login Mobiltelefon

Auslösen:

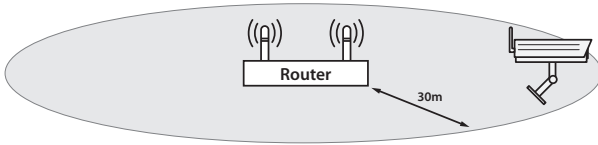
1. Großschreibung.
2. Mobiltelefon (Für Browser die Javascript unterstützen).
3. Bitte laden und installieren Sie das Installations-Plug-in wenn das Video nicht richtig angezeigt wird.

OCX laden

Geben Sie den Benutzernamen und das Passwort erneut ein. Der Zugriff auf die Kamera erfolgt auf die gleiche Weise wie in den Abschnitten „Browserzugriff auf die Kamera“ (S. 25) beschrieben.

MONTAGE

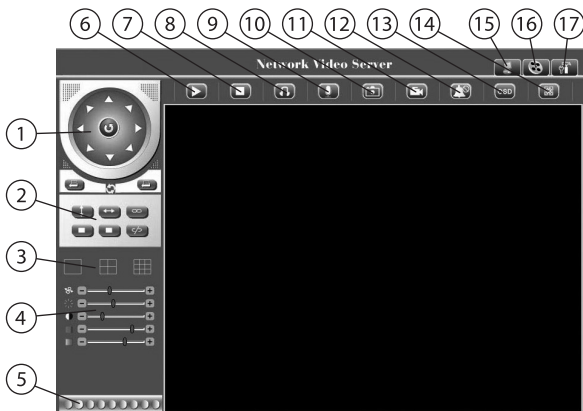
Nachdem die IP-Kamera betriebsbereit ist und in Ihrem Netzwerk erkannt wurde, kann sie aufgestellt werden. Versichern Sie sich, dass die Kamera den von Ihnen gewünschten Bereich überwachen kann und sie sich im Empfangsbereich Ihres WLAN-Routers befindet. Die maximale Reichweite für eine Stabile WLAN-Verbindung beträgt 30 Meter.



VERWENDUNG

GRUNDLEGENDE STEUERUNG


Nach dem Einloggen werden Ihnen das Kamerabild und das Bedienfeld angezeigt. Als Administrator können Sie auf den vollen Funktionsumfang der Kamera zugreifen.



- | | |
|-----------------------|---------------------|
| 6. Steuerungsfeld | 18. OSD-Anzeige |
| 7. Patrouillientasten | 19. Vollbild |
| 8. Multikameraansicht | 20. Standardanzeige |
| 9. Bildeinstellungen | 21. Videowiedergabe |
| 10. Erkannte Kameras | 22. Optionsmenü |
| 11. Live Bildansicht | |
| 12. Bild stoppen | |
| 13. Ton | |
| 14. Lautsprecher | |
| 15. Schnappschuss | |
| 16. Aufnahme | |
| 17. Alarm | |

Von jetzt an werden der von Ihnen festgelegte Benutzername und das neue Passwort benötigt, um über die Login-Seite der IP-Kamera auf diese zuzugreifen.

Login Sprache **Deutsch** ▾

 Anwender

Passwort

Mobiltelefon

Auflösen

1. Großschreibung
2. Mobiltelefon (Für Browser die Javascript unterstützen)
3. Bitte laden und installieren Sie das Installations-Plug-in wenn das Video nicht richtig angezeigt wird.



Geben Sie den gewünschten Anmeldenamen und ein Passwort ein.

Hinzufügen

nwendername

Rechte Administrator ▼

Passwort

Ok Abbrechen

Wählen Sie aus dem Dropdown-Menü die gewünschte Zugangsberechtigung und klicken Sie auf **Bestätigen**.

Besucher	Kann lediglich die aktuelle Anzeige der Kamera betrachten
Anwender	Kann die Anzeige starten/stoppen, Schnapsschüsse machen und Aufzeichnungen starten
Administrator	Hat vollen Zugriff auf alle Einstellungen der Kamera



ACHTUNG:

Im Normalfall sollte nur Ihr eigenes Benutzerkonto über Administrator-Rechte verfügen.

Der neu angelegte Benutzer kann sich jetzt bei der Kamera anmelden.

Login
Sprache Deutsch ▼


Anwender

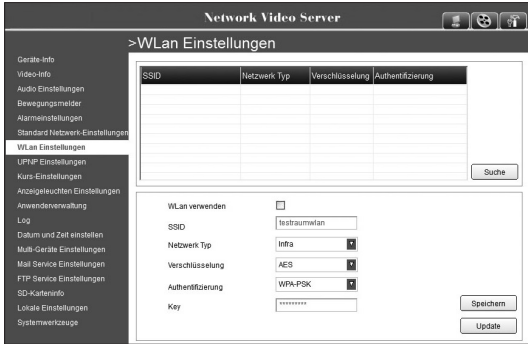
Passwort

Mobiltelefon



WLAN-EINSTELLUNGEN

Die Kamera kann in bestehende WLAN-Netzwerke eingebunden werden. Hierzu muss sie jedoch erst per Kabel mit dem Netzwerk verbunden werden, damit die nötigen Einstellungen vorgenommen werden können. Um zu den Einstellungen zu gelangen, klicken Sie auf  und **WLAN Einstellungen**.



SSID	Netzwerk Typ	Verschlüsselung	Authentifizierung

WLAN verwenden

SSID

Netzwerk Typ

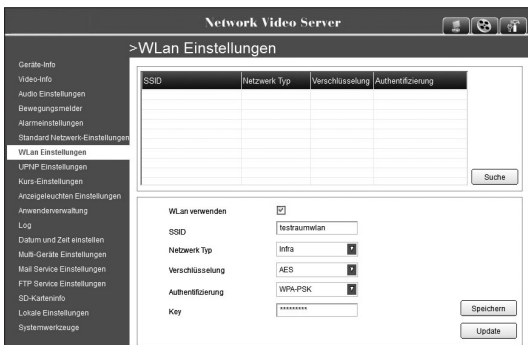
Verschlüsselung

Authentifizierung

Key

Speichern Update

Klicken Sie dann auf den Menüpunkt **Wlan**.



SSID	Netzwerk Typ	Verschlüsselung	Authentifizierung

WLAN verwenden

SSID

Netzwerk Typ

Verschlüsselung

Authentifizierung

Key

Speichern Update

Setzen Sie einen Haken bei **WLAN verwenden**.



HINWEIS:


Da die WLAN-Einstellungen für die Inbetriebnahme der Kamera notwendig sind, werden diese ausführlich im Kapitel „Installation“ (S. 16) behandelt.

MEHRERE KAMERAS IM NETZWERK VERBINDEN

Wenn Sie mehr IP-Kameras der Serie PX-3665-675 und PX-3677-675 verwenden, können Sie bis zu 9 Kameras über ein einzelnes Browserfenster steuern. Richten Sie hierzu zuerst die anderen Kameras wie im Kapitel „Installation“ (S. 16) beschrieben ein und befolgen Sie dann die folgenden Schritte.


Loggen Sie sich auf der gewünschten „Hauptkamera“ ein. Welche IP-Kamera Sie hierfür auswählen, ist nicht relevant. Sie sollten aber nach der Einrichtung immer dieselbe Kamera verwenden oder die folgenden Einstellungen bei jeder Kamera in Ihrem Netzwerk verwenden.

Login Sprache: Deutsch ▾

 Anwender

Passwort

Mobiltelefon

Klicken Sie auf  und wählen Sie den Menüpunkt **Multi-Geräte Einstellungen**.

Network Video Server

>Multi-Geräte Einstellungen

Host	Web Port	Media Port

Id	Host	Web Port	Media Port	Anwendername	Passwort
<input type="checkbox"/>	1	Lokal	--	--	--
<input type="checkbox"/>	2	192.168.1.239	80	admin	*****
<input type="checkbox"/>	3	Keine			
<input type="checkbox"/>	4	Keine			
<input type="checkbox"/>	5	Keine			
<input type="checkbox"/>	6	Keine			
<input type="checkbox"/>	7	Keine			
<input type="checkbox"/>	8	Keine			
<input type="checkbox"/>	9	Keine			



Klicken Sie auf **Zweite Kamera**.

Im Feld **Host**, werden Ihnen die anderen Kameras angezeigt. Mit einem Doppelklick auf die Anzeige wird die IP-Adresse in das Feld unten kopiert. Wenn eine Kamera nicht angezeigt wird, können Sie deren Adresse auch selbst in das Feld **Host** eingeben. Geben Sie den Namen der Kamera unter **Name** ein, falls Sie ihr einen zugewiesen haben. Ansonsten kann dieses Feld auch leer bleiben.

Geben Sie den **http-Port** der Kamera ein. Dieser ist normalerweise 80, wenn Sie ihn nicht manuell umgestellt haben.

Geben Sie den Benutzernamen und das Passwort für das Administrator-Konto der Zielkamera ein. Beachten Sie hierzu auch den Abschnitt „Passwort einstellen“ (S. 45). Klicken Sie zum Abschluss auf **Hinzufügen**.



HINWEIS:

Sie benötigen den Benutzernamen und das Passwort für die Kamera, die Sie verbinden wollen, nicht die Daten für die Kamera die Sie grade verwenden.

Klicken Sie auf **Live Video**. Die Kamera wird jetzt als zusätzlicher grüner Punkt in der unteren Leiste angezeigt.



Sollte eine Kamera nicht erreichbar sein wird der Kreis orange angezeigt.

Wählen Sie eines der Mehrfachansichts-Fenster, um das Bild aller angeschlossenen Kameras zu sehen.

Mit einem Klick in das Kamerabild wechseln Sie in deren Steuerung. Beachten Sie hierzu auch den Abschnitt „Grundlegende Steuerung“ (S. 44). Mit einem Doppelklick in die Anzeige können Sie die Aufnahme als Vollbild anzeigen lassen.



Wiederholen Sie diese Schritte, um bis zu 9 Kameras im Netzwerk miteinander zu Verbinden.



HINWEIS:

Falls Sie sowohl Outdoor- als auch Indoorkameras dieser Serie miteinander verbinden, sollten Sie das Menü einer Indoorkamera für die Steuerung verwenden. Da die Indoorkameras über den Browser bewegt werden können, verfügen diese über ein erweitertes Menü, das bei deren Ansteuerung verwendet werden sollte. Das Steuerungsfeld ist bei der Verwendung mit einer OUTDOOR-IP-Cam ohne Funktion.



UPDATES INSTALLIEREN

Wenn neue Firmware-Versionen verfügbar werden, können Sie diese auf www.pearl.de herunterladen. Diese Updates dienen der Erweiterung des Funktionsumfangs und der Behebung bekannter Fehler.

Bitte befolgen Sie die nachfolgenden Schritte exakt, da sonst kein erfolgreiches Update ausgeführt werden kann.



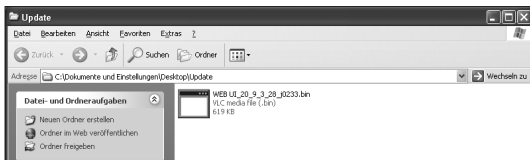
ACHTUNG:

Während des Updates darf die Stromversorgung der Kamera keinesfalls unterbrochen werden.

Klicken Sie links auf **SUPPORT (Treiber & Co.)**. Geben Sie dann die Artikelnummer (PX-3677-675) in das Feld ein und klicken Sie auf **OK**, um die neueste verfügbare Software für Ihre IP-Kamera zu finden.



Speichern Sie die Update-Datei auf dem Desktop Ihres Computers oder in einem neuen Ordner. Es handelt sich um eine **.bin**-Datei. Ändern Sie niemals den Dateinamen, da das Update sonst nicht installiert werden kann.



Starten Sie Ihren Internetexplorer und geben Sie die IP-Adresse Ihrer Kamera ein. Beachten Sie hierzu auch die Hinweise im vorherigen Kapitel. Warten Sie, bis der Login-Schirm angezeigt wird.

Login

Sprache Deutsch

Anwender

Passwort

Login Mobiltelefon

Auflösen

1. Großschreibung
2. Mobiltelefon (Für Browser die Javascript unterstützen)
3. Bitte laden und installieren Sie das Installations-Plug-In wenn das Video nicht richtig angezeigt wird.

OCX laden

Wählen Sie im Browserfenster der Kamera die Option .

Wählen Sie den Punkt **Systemwerkzeuge**.

Network Video Server

>Systemwerkzeuge

Geräte-Info

Video-Info

Audio-Einstellungen

Bewegungsmelder

Alarmeinstellungen

Standard Netzwerk-Einstellungen

WLAN-Einstellungen

UPnP-Einstellungen

Kurs-Einstellungen

Anzeigeleuchten-Einstellungen

Gerät neustarten

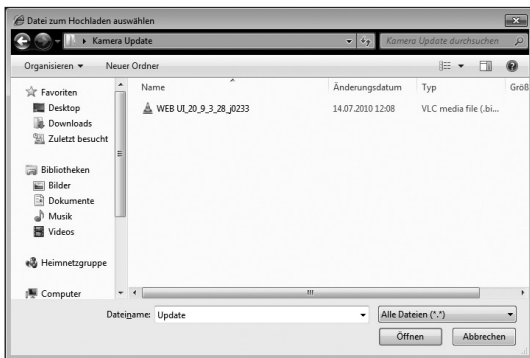
Werkzeinstellungen wiederherstellen

Firmware Upgrade

Interface Upgrade

Wählen Sie die gewünschte Option und klicken Sie auf **Durchsuchen**.

Warten Sie, bis sich das Fenster zur Dateiauswahl öffnet und wählen Sie die Update-Datei. Klicken Sie auf **Öffnen**.



Klicken Sie **Start**.

Die Kamerasoftware versucht nun neu zu starten.

Warten Sie bis der Countdown abgelaufen ist. Starten Sie Ihren Internet Explorer neu und geben Sie die IP-Adresse der Kamera ein. Sie werden vom neuen Anmeldefenster begrüßt. Geben Sie wie gewohnt Ihren Benutzernamen und Ihr Passwort ein.

Die neue Firmware ist jetzt betriebsbereit und kann verwendet werden. Sie können die verwendete Firmware-Version jederzeit überprüfen, indem Sie **Geräte-Info** und den Menüpunkt **Info** klicken.

Network Video Server

>Geräte-Info

Geräte-ID	<input type="text" value="00ea21638202"/>	
Geräte-Client-Version	<input type="text" value="1.12.5.13"/>	
Geräte-Host-Version	<input type="text" value="8.1.5.22"/>	
Beschreibung	<input type="text" value="IP CAMERA"/>	
IP-Adresse	<input type="text" value="192.168.1.155"/>	
UPNP Status	<input type="text" value="Fehlgeladnen"/>	<input type="button" value="Speichern"/>
DDNS Status	Fehlgeladnen http://pearl.endofinternet.net:80	<input type="button" value="Neu laden"/>

Geräte-Info
 Video-Info
 Audio-Einstellungen
 Bewegungsmelder
 Alarmeinstellungen
 Standard Network-Einstellungen
 WLAN-Einstellungen
 UPNP-Einstellungen
 Kurs-Einstellungen
 Anzeigeluchten-Einstellungen
 Anwenderverwaltung
 Log




ACHTUNG:

Die Kamera kann beschädigt werden, wenn diese von der Stromversorgung oder Ihrem Computer getrennt wird, während das Update ausgeführt wird. Bei Schäden, die durch falsche Ausführung des Updates entstehen, entfällt der Gewährleistungsanspruch. Halten Sie sich daher genau an die hier aufgeführten Schritte.

VIDEOAUFNAHMEN

Klicken Sie auf das Kamerasymbol auf dem Hauptbildschirm, um eine Videoaufnahme zu starten. Das Symbol wird grün angezeigt während die Kamera aufnimmt.

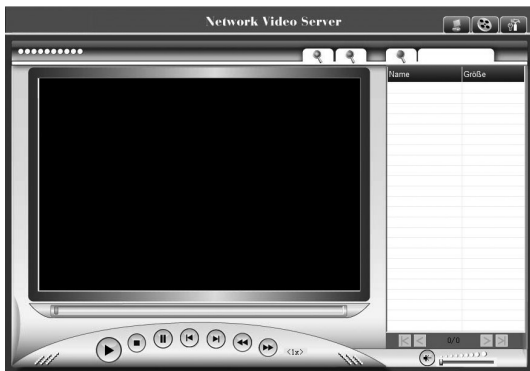


Aufnahmen werden werkseitig auf der microSD-Karte in der Kamera gespeichert. Sie können den Speicherpfad ändern, indem Sie  klicken und den Punkt **Lokale Einstellungen** wählen.



Klicken Sie auf **Durchsuchen**, um einen neuen Speicherpfad in ihrem Netzwerk zu wählen.

Klicken Sie auf , um Videos abzuspielen.




Im Fenster rechts, können Sie die Videodateien aufrufen. Mit dem Tastenfeld unter der Bildanzeige können Sie die Wiedergabe steuern.



HINWEIS:

Wenn die Dateien lokal gespeichert sind, können Sie diese auch direkt auf Ihrem Computer abspielen, ohne die Kamera zu verwenden.

KURS FESTLEGEN

Sie können eine feste Bewegungsabfolge und Abstände einstellen, nach denen die Kamera sich bewegen soll. Klicken Sie für diese Funktion auf .



Network Video Server

>Geräte-Info

Geräte-Info

Geräte-ID: 00ea21638292

Geräte-Client-Version: 1.12.5.13

Geräte-Host-Version: 8.1.5.22

Beschreibung: IP CAMERA

IP-Adresse: 192.168.1.155

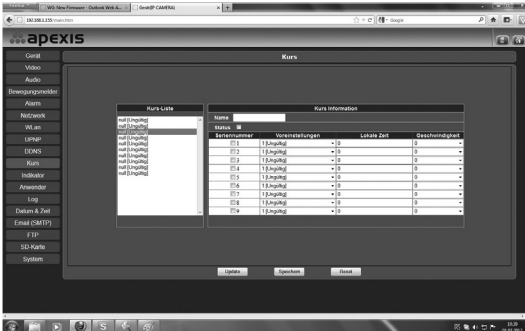
UPnP Status: Fehlgeladungen

DDNS Status: Fehlgeladungen <http://pearl.endofinternet.net/80>

Speichern

Neu laden

Wählen Sie aus dem Menü links die Option **Kurs**.



apexis

Kurs

Kurs Liste

Name	Status
001 (Langzeit)	OK
002 (Langzeit)	OK
003 (Langzeit)	OK
004 (Langzeit)	OK
005 (Langzeit)	OK
006 (Langzeit)	OK
007 (Langzeit)	OK
008 (Langzeit)	OK
009 (Langzeit)	OK

Kurs Information

Name	Parameter	Parameterwert	Letzte Zeit	Geschwindigkeit
001	1	10 (m/s)	10	0
002	2	10 (m/s)	10	0
003	3	10 (m/s)	10	0
004	4	10 (m/s)	10	0
005	5	10 (m/s)	10	0
006	6	10 (m/s)	10	0
007	7	10 (m/s)	10	0
008	8	10 (m/s)	10	0
009	9	10 (m/s)	10	0

OK

Speichern

Abbrechen


Im Kursmenü können Sie die gewünschten Geschwindigkeit und die Zeitabstände für die Kamerabewegungen einstellen.

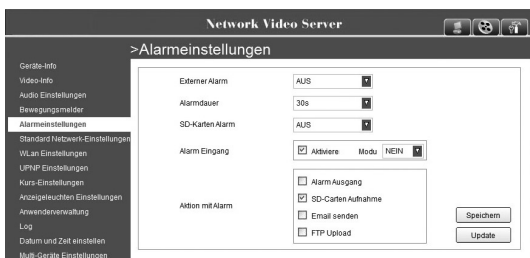
ANHANG

ANSCHLUSS VON BEWEGUNGSMELDERN

An den I/O-Anschlüssen an der Rückseite der Kamera kann ein Bewegungsmelder angeschlossen werden.

Einstellungen des Alarmdienstes

Klicken Sie auf  und wählen Sie **Alarmeinstellungen**, um die Bewegungsmelder-Funktion einzurichten.



The screenshot shows the 'Network Video Server' web interface. The main heading is '>Alarmeinstellungen'. On the left is a navigation menu with options like 'Geräte-Info', 'Video-Info', 'Audio-Einstellungen', 'Bewegungsmelder', 'Alarmeinstellungen', 'Standard Netzwerk-Einstellungen', 'WLAN-Einstellungen', 'UPNP-Einstellungen', 'Kurs-Einstellungen', 'Anzeigeleuchten-Einstellungen', 'Anwenderverwaltung', 'Log', 'Datum und Zeit einstellen', and 'Multi-Geräte-Einstellungen'. The 'Alarmeinstellungen' section contains the following fields:

Edelmer Alarm	AUS
Alarmdauer	30s
SD-Karten Alarm	AUS
Alarm Eingang	<input checked="" type="checkbox"/> Aktiviere Modu: NEIN
Aktion mit Alarm	<input type="checkbox"/> Alarm Ausgang
	<input checked="" type="checkbox"/> SD-Karten Aufnahme
	<input type="checkbox"/> Email senden
	<input type="checkbox"/> FTP Upload

Buttons for 'Speichern' and 'Update' are located at the bottom right of the form.

Setzen Sie einen Haken bei **Alarm Eingang**, um die Funktion zu verwenden.

Wenn die Bewegungserkennung aktiviert wurde können weitere Einstellungen (wie die Empfindlichkeit und die Art des Alarms) festgelegt werden.

I/O Pins

1. Output (+5V)
2. Output
3. Alarm Input
4. Input (GND)





BEISPIEL:

Sie können einen Personen-Infrarot-Sensor (PIP) für die Bewegungsmeldung anschließen. Wenn der externe Sensor ausgelöst wird, kann die IP-Kamera darauf programmiert werden, eine E-Mail mit einem Bild zu senden oder es intern zu speichern.

Wenn Sie einem externen Alarm mit Pin 3 und Pin 4 verknüpfen, dann wird der externe Alarm aktiviert, sobald Sie das Feld bei **Alarm Eingang aktiviert** ausgewählt haben.

I/O Verbindung bei Alarm

Bei Alarm wird die I/O-Verbindung aktiviert. Pin 1 wird als Output bei Auslösen verwendet. Pin 2 wird beim Beenden verwendet.

Mit den Feldern  und  können Sie den Pin 1 (+5 V) manuell steuern.



HINWEIS:

Setzen Sie Haken hinter die gewünschten Alarmreaktionen. Die Kamera kann Bilder als E-Mails versenden, auf dem Computer speichern und auf einen Server laden. Die jeweiligen Einstellungen müssen jedoch bereits in den einzelnen Menüs vorgenommen worden sein.

LÖSUNG HÄUFIGER PROBLEME (TROUBLESHOOTING)

Die Kamera wird im Netzwerk nicht erkannt

1. Überprüfen Sie, ob die IP-Adresse der Kamera im selben Subnetz liegt wie Ihr restliches Netzwerk.
2. Versichern Sie sich, dass die der Kamera zugewiesenen IP- und Mac-Adressen nicht schon an andere Geräte Ihres Netzwerks vergeben sind.
3. Überprüfen Sie Schritt für Schritt die Netzwerkeinstellungen der IP-Kamera.
4. Versichern Sie sich, dass Ihr Router eingehende Signale von Port 80 erlaubt.
5. Überprüfen Sie, ob Ihr Router Port Forwarding aktiviert hat.

Das Passwort und/oder der Benutzername sind verloren gegangen

Die einzige Möglichkeit wieder auf die Kamera zuzugreifen ist die Werkseinstellungen wiederherzustellen. An der Unterseite der Kamera befindet sich eine versenkte Reset-Taste. Verwenden Sie eine Büroklammer oder einen ähnlichen Gegenstand, um diese Taste für mehrere Sekunden zu drücken. Die Kamera wird zurückgesetzt und kann wieder mit dem Benutzernamen „admin“ und ohne Passwort verwendet werden.



ACHTUNG:

Durch das Wiederherstellen der Werkseinstellungen werden alle vorgenommenen Einstellungen gelöscht. Alle Benutzerdaten gehen verloren, die Zugangsdaten zu Ihrem Netzwerk sind gelöscht und die IP-Kamera muss vollständig neu eingerichtet werden. Führen Sie diesen Vorgang daher nicht leichtfertig aus.

Die Bilderübertragungsrate ruckelt und/oder ist von minderer Qualität

Die Übertragung wird von mehreren Faktoren wie der genutzten Bandbreite, der Anzahl der IP-Kameras, der Prozessorleistung Ihres Computers, der Anzahl der Zugriffe, von Störsignalen im WLAN (auf der 2,4 GHz Frequenz) und durch die Modus- und Helligkeitseinstellungen beeinflusst. Überprüfen Sie, ob einer dieser Faktoren ungewöhnlich hoch oder niedrig ist, um das Problem zu identifizieren. Fall Ihr Netzwerk Hubs verwendet, tauschen Sie diese durch Netzwerk-Switches aus, um eine bessere Übertragung zu sichern.

Da bei Netzwerken häufig Unklarheiten und missverständliche Begriffe auftreten, soll dieses Glossar dabei helfen, Licht ins Dunkel mancher Fachbegriffe zu bringen. Im Folgenden werden die grundlegenden Hardwarekomponenten eines herkömmlichen Heimnetzwerks ebenso dargestellt wie die verwendeten Anwendungen und Dienste.

Hardware

- **Access-Point**
Der Zugangspunkt oder auch Access-Point ist die „Basisstation“ in einem drahtlosen Netzwerk (WLAN). Diese Funktion wird häufig in Heimnetzwerken auch von einem Router übernommen.
- **DSL-Modem**
Das DSL-Modem verbindet Ihren Computer mit dem Internet. Wenn Sie mit mehr als einem Computer über eine Leitung Zugriff auf das Internet haben wollen, benötigen Sie einen Router, der direkt hinter das DSL-Modem geschaltet wird.
- **Kabelmodem**
Als Kabelmodem bezeichnet man das Gerät, das Daten über Fernseh-Kabelnetze überträgt und für Breitband-Internetzugänge über Kabelanschlüsse (Kabelinternet) eingesetzt wird.
- **Netzwerkkabel/Ethernetkabel**
Hier gibt es zwei Varianten, so genannte „Patch“-Kabel und „Crossover“-Kabel. Patchkabel sind die Kabel, die am häufigsten Verwendung in Netzwerken finden. Sie werden eingesetzt um Computer mit Switches oder Routern zu verbinden. Crossover-Kabel werden dazu eingesetzt, um zwei Computer direkt miteinander zu verbinden, ohne ein Netzwerk zu verwenden. Patchkabel sind der gängige Lieferumfang von Netzwerkprodukten.

- **Netzwerkswitch**

Switches werden als „Knotenpunkt“ von Netzwerken eingesetzt. Sie dienen dazu, mehrere Netzwerkgeräte „auf ein Kabel“ im Netzwerk zusammenzuführen. Switches sind häufig zu logischen Verbänden zusammengestellt und verbinden z.B. alle Computer aus einem Büro. Koppelt man mehrere Switches, erhält man ein komplexeres Netzwerk, das einer Baumstruktur ähnelt.

- **Router**

Router dienen zur Zugriffssteuerung von Netzwerkcomputern untereinander und regeln ebenfalls den Zugriff auf das Internet für alle im Netzwerk befindlichen Computer. Router werden sowohl rein kabelgebunden als auch als WLAN-fähige Variante vertrieben. Meist übernehmen handelsübliche Router noch Sonderfunktionen wie z.B. DHCP, QoS, Firewall, NTP,...

Grundlegende Netzwerkbegriffe

- **Adressbereich**

Ein Adressbereich ist eine festgelegte Gruppe von IP- oder MAC-Adressen, fast diese zu einer „Verwaltungseinheit“ zusammenfasst.

- **Blacklist**


Mit einer Blacklist bezeichnet man bei Netzwerken eine Liste von Geräten, denen die Verbindung zu einem Gerät (z.B. Router) explizit nicht erlaubt ist. Alle anderen Geräte werden von dem Gerät akzeptiert, das den Zugang über die Blacklist regelt. Im Gegensatz dazu steht die so genannte Whitelist.

- **Browser**


Browser werden Programme genannt, die hauptsächlich zur Darstellung von Webseiten genutzt werden. Die bekanntesten Browser sind Internet Explorer, Mozilla Firefox, Opera oder Google Chrome.



- **Client**

Als Client wird jede Anwendung bezeichnet, die Daten eines Serverdienstes in Anspruch nimmt. Eine klassische Client-Server Bindung entsteht in Heimnetzwerken häufig schon bei der Vergabe von IP-Adressen im Netzwerk. Hier fordert der Computer als DHCP-Client  eine gültige IP-Adresse vom DHCP-Server (meist der Router) an und erhält diese vom DHCP-Server zugeteilt.

- **IP-Adresse**

IP-Adressen werden dazu verwendet Computer, Drucker oder andere Geräte flexibel in ein Netzwerk einzubinden. Hierbei ist zwischen globalen und privaten IP-Adressen zu unterscheiden. Globale IP-Adressen werden von den einzelnen Internet-Anbietern oftmals dynamisch (DHCP ) vergeben. Sie dienen dazu, Ihr Heimnetzwerk oder auch nur den einzelnen Computer gegenüber dem Internet erreichbar zu machen. Private IP-Adressen werden im Heimnetzwerk entweder statisch („von Hand“) zugewiesen oder dynamisch (DHCP) vom Anwender selbst vergeben. IP-Adressen ordnen ein spezielles Gerät eindeutig einem bestimmten Netzwerk zu.




Beispiel:

IP-Adressen sind die bekanntesten Adressierungen im Netzwerk und treten in folgender Form auf:
192.168.0.1

- **ISP**

ISP ist die Abkürzung für „Internet Service Provider“. Dieser Begriff wird für Stellen verwendet, die einem Netzwerk oder Einzelcomputer den Zugang zum Internet anbieten. In Deutschland ist der wohl bekannteste ISP T-Online, aber auch Anbieter wie Freenet, Arcor, 1&1 oder KabelDeutschland gehören zu den ISPs.


- **LAN**

LAN (Local Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über einen gemeinsamen Adressbereich  verfügen und damit zu einer Struktur zusammengefasst werden.







- **Passphrase**



Mit dem Begriff Passphrase wird ein Schlüsselwort oder -satz umschrieben, der als Sicherheitsabfrage bei der Verbindung zu WPA-/WPA2-verschlüsselten  Netzwerken eingegeben werden muss.

- **Port**

Als Port wird eine Softwareschnittstelle bezeichnet, die es einzelnen Anwendungen auf Ihrem Computer ermöglicht, mit den Anwendungen eines Anbieters zu kommunizieren. Hier wird hauptsächlich zwischen zwei Protokollen unterschieden: TCP  und UDP .





Beispiel:

Die häufigste Internet Anwendung ist ein Browser  (Internet Explorer, Mozilla Firefox, usw.), der meist über den TCP-Port 80 mit den Servern  der Webseiten-Anbieter kommuniziert.





- **Protokoll**

Protokolle im Netzwerk sind Standards für Datenpakete, die Netzwerkgeräte untereinander austauschen, um eine eindeutige Kommunikation zu ermöglichen.

- **Pre-Shared Key**

Mit Pre-Shared Key („vorher vereinbarter Schlüssel“) oder kurz PSK bezeichnet man ein Verschlüsselungsverfahren , bei denen die verwendeten Schlüssel vor der Verbindung beiden Teilnehmern bekannt sein müssen (siehe auch WPA/WPA2 .

- **MAC-Adresse**

Als MAC-Adresse bezeichnet man die physikalische Adresse einer Netzwerkkomponente (z.B. Netzwerkkarte , WLAN-Dongle , Drucker, Switch ). MAC-Adressen sind entgegen IP-Adressen  immer eindeutig zuordenbar. MAC-Adressen von anderen verbundenen Netzwerkgeräten werden von den einzelnen Geräten jeweils in einer so genannten ARP-Tabelle gespeichert. Diese ARP-Tabellen können zur Fehlersuche dienen, falls ein Gerät ohne IP-Adresse (z.B. Switch) im Netzwerk keine Funktion zeigt.





Beispiel:


Eine MAC-Adresse sieht z.B. so aus: 00:00:C0:5A:42:C1

- **Sichere Passwörter**


Unter sicheren Passwörtern versteht man Passwörter, die bestimmte Bedingungen erfüllen, um von Angreifern nicht mit einfachsten Mitteln entschlüsselt werden zu können.

Sichere Passwörter sollten generell eine bestimmte Mindestlänge aufweisen und mehrere Sonderzeichen beinhalten. Als Faustregel gilt hier: Je länger das Passwort ist und je mehr Sonderzeichen es beinhaltet, desto sicherer ist es gegen Entschlüsselung.


- **SSID**

SSID (Service Set Identifier) steht für die Bezeichnung, die für ein WLAN-Netzwerk verwendet wird. Diese SSID wird meist per Broadcast (siehe UDP ) öffentlich ausgesendet, um das Netzwerk für mobile Geräte „sichtbar“ zu machen.

- **Subnetz**


Subnetze sind eine Zusammenfassung von einzelnen IP-Adressen  zu Netzwerkstrukturen. So werden meist Computer einer Abteilung im Büro in einem Subnetz zusammengefasst, während die Computer einer anderen Abteilung in einem weiteren Subnetz zusammengefasst sind. Daher sind Subnetze eine reine Strukturierungsmaßnahme. Eine Angabe des Subnetzraumes wird immer in Zusammenhang mit der Vergabe einer IP-Adresse durchgeführt. Im Heimbereich werden normalerweise keine speziellen Subnetze eingerichtet. Daher ist bei Windows-Systemen als Subnetzmaske die 255.255.255.0 voreingestellt. Dadurch stehen die IP-Adressen xxx.xxx.xxx.1 bis xxx.xxx.xxx.254 zur Verfügung.

- **TCP (Transmission Control Protocol)**

Das TCP-Protokoll wird dazu verwendet, gezielt Informationen von einem speziellen Gegenüber abzufragen (siehe Beispiel bei Port )


- **UDP (User Datagram Protocol)**
Das UDP-Protokoll ist ein so genanntes „Broadcast“-Protokoll. Broadcast wird im Englischen auch für Radio- oder TV-Sendungen verwendet. Ganz ähnlich arbeitet dieses Protokoll. Es wird verwendet, um Datenpakete an alle im Netzwerk erreichbaren Geräte zu senden und im Weiteren auf Rückmeldung dieser Geräte zu warten. Das UDP-Protokoll wird meist dann von Anwendungen eingesetzt, wenn unsicher ist, ob eine entsprechende Gegenstelle im Netzwerk vorhanden ist.
- **uPNP**
Mit diesem Begriff wird das „universal Plug and Play“-Protokoll bezeichnet. Dieses Protokoll wird hauptsächlich dazu verwendet, Drucker und ähnliche Peripheriegeräte über ein Netzwerk ansteuern zu können.
- **Verschlüsselung**
Verschlüsselungsmechanismen werden in Netzwerken dazu eingesetzt, Ihre Daten vor fremdem Zugriff abzusichern. Diese Verschlüsselungsmechanismen funktionieren ähnlich wie bei einer EC-Karte. Nur mit dem richtigen Passwort (der richtigen PIN) können die Daten entschlüsselt werden.
- **VPN**
VPN (Virtual Private Network) steht für eine Schnittstelle in einem Netzwerk, die es ermöglicht, Geräte an ein benachbartes Netz zu binden, ohne dass die Netzwerke zueinander kompatibel sein müssen.
- **WAN**
WAN (Wide Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über größere Entfernungen und aus vielen Bestandteilen zusammengefasst werden. Das bekannteste Beispiel ist das „Internet“, jedoch kann ein WAN auch nur aus zwei räumlich voneinander getrennten LANs bestehen.

- **Whitelist**

Mit einer Whitelist bezeichnet man bei Netzwerken eine Liste von Geräten, denen die Verbindung zu einem Gerät (z.B. Router) explizit erlaubt ist. Alle anderen Geräte werden von dem Gerät abgewiesen, das den Zugang über die Whitelist regelt. Im Gegensatz dazu steht die so genannte Blacklist .

Dienste in Netzwerken

- **DHCP (Dynamic Host Configuration Protocol)**



Mit DHCP wird die dynamische Verteilung von IP-Adressen  in Netzwerken bezeichnet. Dynamisch sind diese Adressen deshalb, weil Sie jederzeit ohne größeren Aufwand neu vergeben werden können. Man kann dynamische IP-Adressen auch als geliehene IP-Adressen bezeichnen. Diese geliehenen IP-Adressen werden mit einem „Verfallsdatum“ versehen – der so genannten „Lease Time“. Ein Computer wird am DHCP-Server nur dann nach einer neuen IP-Adresse anfragen, wenn sein „Lease“ abgelaufen ist. Dies ist allerdings auch eine mögliche Fehlerquelle, da es hier zu Unstimmigkeiten zwischen DHCP-Server und DHCP-Clients kommen kann.



HINWEIS:

Windows Computer sind standardmäßig als DHCP-Client eingestellt, um einen einfachen Anschluss an ein Heimnetzwerk zu ermöglichen.




- **DNS (Domain Name Server)**

DNS ist ein Serverdienst, der die Übersetzung von IP-Adressen  in gängige Internet-Adressen übernimmt. So wird z.B. aus www.google.de die IP-Adresse: 74.125.39.105. Werden Sie während einer Konfiguration aufgefordert, die DNS-IP-Adresse einzugeben, ist damit immer die Adresse desjenigen Servers  gesucht, der den DNS-Serverdienst anbietet. DNS-Server werden aus Gründen der Ausfallsicherheit meist doppelt angegeben und als Primärer DNS (oder DNS1) bzw. Sekundärer DNS (oder DNS2) bezeichnet.

- **Filter**

Siehe auch Firewall 




- **Firewall**

Eine Firewall ist ein Sicherungsmechanismus, der meist auf Routern  als Serverdienst läuft, jedoch bereits in Windows (seit XP) integriert ist. Sie erlaubt nur Zugriffe auf voreingestellte Ports , blockt vorher konfigurierte IP-Adressen  und soll generell schädliche Angriffe auf Ihr Netzwerk verhindern.

- **FTP/NAS (File Transfer Protocol/ Network Access Storage)**

FTP ist ein Serverdienst, der hauptsächlich zum Transfer von Dateien verwendet wird. Dieser Dienst ermöglicht es auf unkomplizierte Art und Weise Dateien von einem Computer auf einen entfernt stehenden anderen Computer ähnlich dem Windows Explorer zu übertragen. So genannte NAS-Server setzen ebenfalls häufig diesen Dienst ein, um einen Zugriff aus dem gesamten Netzwerk auf eine Festplatte zu erlauben.




- **(Standard-) Gateway**

Als Gateway wird die Schnittstelle bezeichnet, die es den Computern im privaten Netzwerk ermöglicht mit Computern außerhalb zu kommunizieren. Es ist in diesem Sinne mit Ihrem Router  gleichzusetzen. Das Gateway sammelt und sendet Anfragen der Clients  und leitet diese weiter an die entsprechenden Server  im Internet. Ebenso verteilt das Gateway die Antworten der Server wieder an die Clients, die die Anfrage gestellt hatten.


- **HTTP/Webserver (Hypertext Transfer Protocol)**

Dieser Dienst ist das, was in der Öffentlichkeit als „Das Internet“ bezeichnet wird. Jedoch handelt es sich hier bei nur um eine Vereinfachung, da das Internet an sich eine übergeordnete Struktur ist, die nahezu alle Serverdienste beinhaltet. HTTP wird zum Transfer und der Darstellung von Webseiten verwendet.



- **Mediastreams**

Diese Gruppe von Serverdiensten wird von vielfältigen Geräten und Anbietern verwendet. Die bekanntesten Beispiele sind Internet-Radiosender, Video-On-Demand und IP-Kameras. Diese Streams nutzen teils unterschiedliche Protokolle  und Protokollversionen. Daher kann es hier durchaus einmal zu Inkompatibilitäten zwischen Server  und Client  kommen.

- **NTP**

NTP (Network Time Protocol) bezeichnet ein Protokoll , mit dem Computer über das Netzwerk ihre Datums- und Zeiteinstellungen abgleichen können. Dieser Dienst wird von weltweit verteilten Servern bereitgestellt.

- **PPPoE**

PPPoE steht für PPP over Ethernet und bezeichnet Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird in Deutschland hauptsächlich in Verbindung mit ADSL-Anschlüssen verwendet. ADSL bedeutet Asynchrones DSL und steht für die Verwendung einer Leitung für Telefon und Internet. ADSL ist Standard in Deutschland. Hauptgrund für die Verwendung von PPPoE ist die Möglichkeit, Authentifizierung und Netzwerkkonfiguration (IP-Adresse , Gateway ) auf dem schnelleren Ethernet zur Verfügung zu stellen.

- **Samba/SMB**

Mit diesen Begriffen ist ein Serverdienst gemeint, der speziell in Windows Netzwerken verwendet wird. Dieser Service ermöglicht ebenfalls den schnellen und einfachen Zugriff auf Dateien die sich auf anderen Computern befinden (in so genannten „freigegebenen Ordnern“). Jedoch ist dieser Dienst auf Heimnetzwerke begrenzt und kann nur in Ausnahmefällen auch über das Internet in Anspruch genommen werden.

- **Server/Serverdienst**

Ein Server ist immer als Anbieter von Netzwerkdiensten zu sehen. Einzelne Anwendungen werden auch als Serverdienst bezeichnet. Die bekanntesten Serverdienste sind Webserver, DHCP oder E-Mail Server. Mehrere solche Dienste können auf einem Computer oder anderen Geräten (z.B. Routern) gleichzeitig verfügbar sein. Server werden auch Computer genannt, deren ausschließliche Funktion darin besteht Serverdienste anzubieten und zu verwalten.

- **Statische Adressvergabe**

Bei der statischen Adressvergabe sind alle Netzwerkadressen eines Netzwerkes fest vergeben. Jeder einzelne Client (Computer) des Netzwerks hat seine feste IP-Adresse, die Subnetzmaske, das Standard-Gateway und den DNS-Server fest eingespeichert und muss sich mit diesen Daten beim Server anmelden.

Ein neuer Client (Computer) muss erst mit einer gültigen, noch nicht vergebenen IP-Adresse und den restlichen Daten ausgestattet werden, bevor er das Netzwerk nutzen kann. Manuelle Adressvergabe ist besonders bei Netzwerkdruckern oder ähnlichen Geräten sinnvoll, auf die häufig zugegriffen werden muss, oder in Netzwerken, die besonders sicher sein müssen.

- **WEP und WPA**

Wired Equivalent Privacy (WEP) ist der ehemalige Standard-Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln als auch die Vertraulichkeit der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen. Daher sollten WLAN-Installationen die sicherere WPA-Verschlüsselung verwenden. Wi-Fi Protected Access (WPA) ist eine modernere Verschlüsselungsmethode für ein WLAN. Sie wurde als Nachfolger von WEP eingeführt und weist nicht deren Schwachstellen auf.

SICHERHEITSMASSNAHMEN IN WLAN-NETZWERKEN

An erster Stelle sollten der Verzicht von WEP und der Einsatz von WPA oder WPA2 stehen. Dieses Ziel lässt sich in vielen Fällen bereits durch ein Treiber- oder Firmwareupdate erreichen. Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende grundlegende Behelfsmaßnahmen beachtet werden, um das Risiko von Angriffen fremder Personen auf das WLAN zu minimieren:

- Aktivieren Sie auf alle Fälle den Passwortschutz! Ändern Sie ggf. das Standard-Passwort des Access Points.
- Wenn Sie die WEP-Verschlüsselung verwenden, weil eines der angeschlossenen Geräte WPA oder WPA2 (dringend empfohlen) nicht unterstützt wird, sollte der WEP-Schlüssel mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen darstellen.
- Aktivieren Sie die Zugriffskontrollliste (ACL = Access Control List), um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen. Beachten Sie, dass sich eine MAC-Adresse aber mittels Treiber beliebig einstellen lässt, sodass eine mitgelesene zugelassene MAC-Adresse leicht als eigene ausgegeben werden kann.
- Verwenden Sie eine sinnvolle SSID: Die SSID des Access Points sollte keine Rückschlüsse auf Ihren Namen, verwendete Hardware, Einsatzzweck und Einsatzort zulassen.
- Umstritten ist die Deaktivierung der SSID-Übermittlung (Broadcasting). Sie verhindert das unabsichtliche Einbuchten in das WLAN, jedoch kann die SSID bei deaktiviertem Broadcasting mit einem so genannten Sniffer (Gerät zur LAN-Analyse) mitgelesen werden, wenn sich etwa ein Endgerät beim Access Point anmeldet.
- WLAN-Geräte (wie der Access Point) sollten nicht per WLAN konfiguriert werden, sondern ausschließlich über eine kabelgebundene Verbindung.
- Schalten Sie WLAN-Geräte stets aus, wenn Sie sie nicht benutzen.
- Führen Sie regelmäßige Firmware-Updates vom Access Point durch, um sicherheitsrelevante Aktualisierungen zu erhalten.

- Beeinflussen Sie die Reichweite des WLANs durch Reduzierung der Sendeleistung bzw. Standortwahl des WLAN Gerätes (Dies dient allerdings nicht der aktiven Sicherheit, sondern begrenzt lediglich den möglichen Angriffsbereich.)

All diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinwegtäuschen, dass sie letztlich keinen wirklichen Schutz beim Einsatz von WEP bedeuten. Ein erfolgreicher Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 Minuten mit ziemlicher Sicherheit erfolgreich.

CHECKLISTE FÜR DIE KONFIGURATION

Aufgabe	Erledigt
Funkkameraüberwachung ausschalten	
Schnurlostelefon ausschalten	
Sonstige Geräte mit 2,4 GHz ausschalten	
Stromversorgung mit Überspannungsschutz sichern	
Firewall am Computer ausstellen	
Virens Scanner am Computer ausschalten	
MAC-Adressenfilter am vorhandenen Router ausschalten	

Notwendige Daten	Kommentar
Netzwerk SSID	
IP – Gateway	
IP – DNS-Server	
DHCP Range	
Subnetzmaske	
IP – Internetzugang	
IP – Timeserver (wenn vorhanden)	
Passwort – Internetzugang	
Passwort – WLAN	
IPs von vorhandenen Servern (wenn vorhanden)	
IP – Watchdog (wenn vorhanden)	
IP – Log-Server (wenn vorhanden)	
IP – virtuelle DMZ (wenn vorhanden)	



