TecTime Magazin

Ausgabe 11

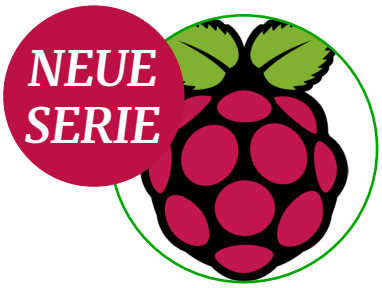
Gewinnspiel für alle Abonnenten

Überraschungspaket von VU+ !

TEST
Gigablue UHD
UE 4K Cable

VORSICHT ABZOCKE
DigiTennaMax

SDR-Projekte
AIRSPY
Kurzvorstellung



Raspberry Pi Serie
Raspberry Pi
als VPN-Server

Gefährliche Apps
in Mediaplayern

8 digitale Technologien, die den Urlaub noch besser machen

INHALT

EDITORIAL

Christian Mass

Chefredakteur

Liebe Leser,

Ein Leser des TecTime Magazins ist chronisch krank und um für Notfälle gewappnet zu sein, schaffte er sich vor zwei Jahren einen GPS-Tracker mit eingebautem Mikrofon an. So wollte er sicherstellen, dass er im Notfall Hilfe bekommt, ohne den unmöglichen Weg zum Telefon. Der GPS Tracker wurde legal erworben und war in Deutschland zugelassen. Ein paar Monate gab es eine neue Verordnung und plötzlich war das Gerät nicht mehr zugelassen. Die Bundesnetzagentur forderte unseren Leser auf entweder das Mikrophon zu entfernen oder das Gerät zu zerstören. Als er nicht sofort reagierte schickte ihm ein eifriger Staatsanwalt die Polizei (drei Beamte mit der Lizenz die Haustür gewaltsam zu öffnen) mit einem Durchsuchungsbeschluss ins Haus. (mehr dazu in der nächsten Ausgabe des TecTime-Magazins).

In der selben Zeit wurde in der durch Lidl vertriebenen Küchenmaschine „Monsieur Cuisine Connect" ein nicht dokumentiertes verstecktes Mikrofon entdeckt. Auch einige moderne Flachbildschirme sind mit geheimen Mikrophonen bestückt. Hinzu kommt noch eine Unmenge von Netzschaltern und Alarmanlagen hinzu. So lauschte Googles Net Guard 18 Monate bis Google unter Druck das Mikrofon dokumentierte.

Unser Leser hat bewusst den GPS-Tracker mit Mikrofon erworben, da er es im Notfall nutzen wollte. Ich nutze den Echo-Lautsprecher und weiß, dass ein Mikro verbaut ist. Ich weiß aber auch das der Echo tatsächlich inaktiv beleibt, solange der Besitzer ihn nicht mit dem Befehl „Alexa" aktiviert. Die Funkstille im Standby-Modus konnten wir in TecTime TV im Frühjahr 2017 belegen.

Wo bleiben eigentlich die Dursuchungsbeschlüsse und Beschlagnahmen der Staatsanwaltschaften für die Standorte der oben beschriebenen Geräte und bei den Anbietern?

Kleine Hilfestellung für die Staatsanwaltschaften: auf www.shodan.io entdecken Sie undokumentierte Mikrofone, Kameras vielen andere mehr. Alles mit Herstellernamen und IP-Adresse des Nutzers. Viel Spaß!

Herzlichst,

Euer Dr.Dish

Impressum

Herausgeber, Chefredakteur und verantwortlich für den Inhalt

Christian Mass | mass@tectime.tv | Naupliaalle. 22, 85521 Ottobrunn

Mehr als nur ein Kabel-Receiver

Gigablue UHD UE 4K Cable

Kabelreceiver sollten billig sein. Das ist eine weit verbreitete Meinung, doch was ist, wenn man sich im Laufe der Zeit entscheidet Sender via DVB T2 oder via Satelliten zu empfangen? Dann ist ein Neukauf nötig und schon wird die Sache teuer. Und warum sollte ein Kabelreceiver nicht denselben Komfort aufweisen, den Linux-Receiver für den Satelliten-Empfang bieten.
Ein solcher Receiver ist der Gigabblue UHD UE 4K Cable.
Wird eine andere Empfangsart gewünscht, so lässt sich diese Set Top Box innerhalb von ein paar Minuten und ohne technisches Wissen zusätzlich auf DVB-S2, DVB-S2X, DVB-T/T2 oder DVB-C/C2 Twin Tuner umrüsten.
Hinzu kommt das Linux-Betriebssystem, dass zahllose und kostenlose add ons bietet. So zum Beispiel IPTV und Streamingdienste.

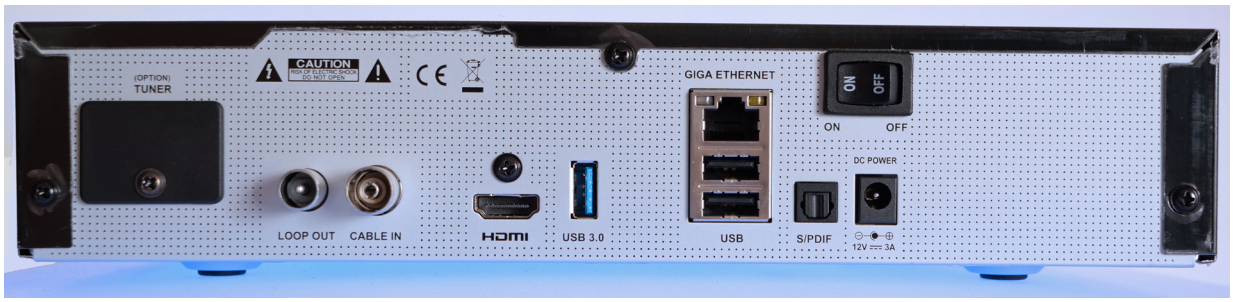
Anmutung und Ausstattung

Nach vielen kleinen Plastik-Receivern tut es gut einen gut verpackten Receiver in den Händen zu halten. Das Metallgehäuse ist sauber verarbeitet und das unauffällige Design passt sich jeder Wohnumgebung gut an.

Mitgeliefert werden das externe Netzteil, die Fernbedienung, 2 AA-Batterien und das Kabel-Set für den nachträglichen Einbau einer 2,5 Zoll Festplatte.

Die Vorderseite des Gigabblue UHD UE 4K Cable wird von einem LCD-Farbdisplay (2,2“) beherrscht. Es zeigt das laufende Programm oder die Menü-Parameter an. Im Standby-Modus lässt sich hier eine hübsche analoge Uhr darstellen. Unter einer Klappe befinden sich zwei Smartcard-Reader, ein Einschub für ein CI-Modul, USB 2.0 Port und die Bedienelemente für Arbeiten direkt am Gerät. Und natürlich die Standby-Taste.

Auf der Rückseite befindet sich die Ein – und Ausgänge des verbauten DVB C/C2 FBC Tuners. Dieser erlaubt die Aufzeichnung von bis zu acht Programmen und die Picture in Picture Darstellung von vier Sendern. Und das mit nur einem Antennenkabel. Links neben dem Tuner gibt es den Steckplatz für die Aufrüstung mittels weiterer Tuner für den Sat-Empfang oder terrestrisches TV. Die Verbindung zum Flachbildschirm schafft der HDMI-Port. Zwei weitere USB 2.0 Ports und ein USB 3.0 Port befinden sich ebenfalls hier. Eine externe Sound Anlage wird über den optischen Audioausgang gefüttert. Das Netzteil findet hier seinen Anschluss und der Netzschalter trennt das Gerät vom Stromnetz.



Die Fernbedienung ist trotz der vielen Funktionen übersichtlich gestaltet. Über sie wird nicht nur der Gigabblue UHD UE 4K Cable gesteuert, sondern auf Wunsch auch noch der Flachbildschirm, ein DVD/Bluray-Player und ein weiteres Gerät.

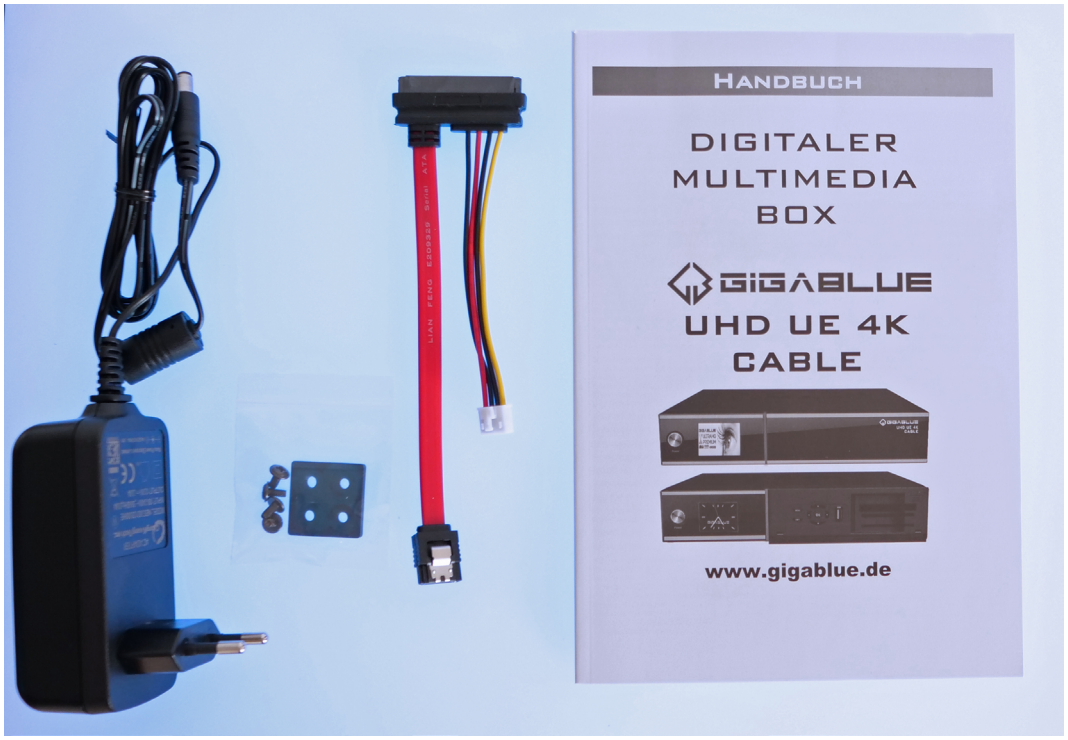
In der Praxis

Die Erstinstallation ist Dank eines Wizzards denkbar einfach. Beim Sendersuchlauf kann man zwischen manuell oder automatisch wählen. Auch die Internetanbindung über die LAN-Schnittstelle funktioniert problemlos. Wer WLAN bevorzugt, der kann einen optionalen WLAN-Stick erwerben. Um den Gigabblue UHD UE 4K Cable voll auszureizen, ist die Internetanbindung ein MUSS.

Hat man die Erstinstallation hinter sich, überraschen zwei Dinge: die extrem kurzen Umschaltzeiten und die hervorragende Bildqualität. Um die volle Bildschirmauflösung genießen zu können, ist leider der optionale Ultra HD Satelliten-Tuner nötig. Und natürlich eine geeignete Antenne.

Ein Tipp für alle Leser mit Antennenverbot: der Fachhandel bietet heute kleine und doch leistungsfähige Sat-Antennen an, die als solche kaum zu erkennen sind. Die umfangreichen Features des Gigabblue UHD UE 4K Cable lassen sich durch kostenlose Plugins erheblich erweitern. Hier sei vor allen Dingen HbbTV, Sat>IP für die Verteilung der Inhalte im eigenen Netzwerk und der Gigablue Player genannt.

Der EPG (elektronischer Programmführer) schafft eine Übersicht über Programme und deren Inhalte für eine Woche. Über den EPG können Inhalte



zur Aufzeichnung im Timer festgelegt werden. Natürlich muss dann eine Festplatte eingebaut sein, oder am USB-Port hängen. Und dann funktioniert auch die Time-Shift Funktion.

Fazit

Der Gigablue UHD UE 4K Cable bietet in der Grundausstattung den Zugang zu Kabelinhalten. Durch die optionalen Tuner ist zukunftssicher.

Die Verarbeitungsqualität und die zahlreichen Features heben ihn deutlich von vielen Wettbewerbern ab.

Features

- Schneller Prozessor mit 2GB DDR4 RAM
- 4GB eMMC Flash
- 2.2" LCD Farbdisplay
- 3 USB (1 vorne + 2 hinten)
- 1 x Ci
- 2 x Smart Card
- 1 x HDMI 2.0
- FBC (DVB-C/C2)
- PnP Gigablue Single DVB-S2x Tuner v.2 (Optional)
- PnP Gigablue Dual DVB-S2x Tuner v.2 (Optional)
- PnP Gigablue Single DVB-C/T2 Tuner v.2 (H. 265) (Optional)
- PnP Gigablue Twin DVB-C/T2 Tuner v.2 (H.265) (Optional)
- Optischer Audioausgangl
- Ethernet Gigabit LAN (RJ-45/1000Mbps)
- 4 x PiP
- SAT>iP, Multiroom Serverfunktion bis zu 16 Klienten

Vorsicht Abzocke

DigiTennaMax

Neuste Technologie

Entworfen mit geheimer Militärtechnik, um 1080 HD-Signale zu empfangen.

Wer kennt sie nicht, die teils aggressive Werbung für eine wahre Wunderantenne. Seit einigen Jahren wird sie unter verschiedenen Namen und Preisen vermarktet. Immer wenn die Produktnamen einen mehr als schlechten Ruf bekommen (FreeSeeTV, TV Radius oder TV Fox), wird gibt es schnell einen neuen Namen.

Zurzeit ist es die DigiTennaMax. Und um deren Google-Werbung kommt man kaum herum. Selbst auf den Homepages einiger Fachzeitschriften im Bereich Satellit und Kabel tauchen sie regelmäßig auf.

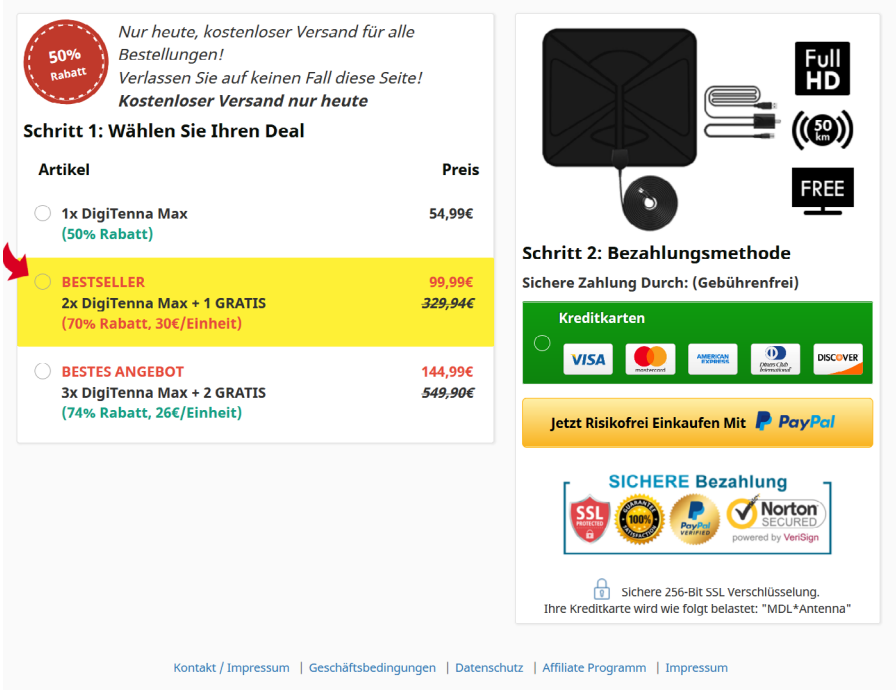
Dem Laien wird vorgegaukelt, das Produkt sei das Ergebnis geheimer Militärtechnik und es sei langlebig, kraftvoll und von hoher Qualität.

Aber vor allen Dingen heißt es der freie Empfang von hunderten HD Sendern überall auf der Welt sein gesichert. Ohne Abo oder Kabelgebühren.

Das alles Dank der Offenlegung geheimer Frequenzen auf denen die Kabelanbieter verpflichtet sind Ihr Programm terrestrisch zusätzlich abzustrahlen. Diese niedrigen Frequenzen mache sich die DigiTennaMax zunutze. Das mit den geheimen Frequenzen der Kabelgesellschaften ist natürlich Blödsinn. **Es gibt sie nicht!** Die hochgelobte Antenne greift einfach auf den DVB T2-Empfang zurück. Soll heißen, sie versucht es zumindest. Und damit die ganze Sache glaubhafter erscheint, listet der Anbieter eine ganze Reihe von Zuschriften glücklicher Besitzer dieser Wunderantenne.

Lässt sich nun ein Interessent von all dem blenden und schreitet zur Bestellung, dann wird Zeitdruck aufgebaut, denn auf der Seite erscheint eine Zeitanzeige, die ihm sagt in xx Minuten sei der Sonderpreis ungültig und somit werde die Antenne teurer. Im Bestellformular ist vom Anbieter schon einmal die Bestellung von zwei Antennen eingekreuzt und so mancher fällt in der Eile darauf hinein. Bezahlt werden die rund 55 Euro pro Stück mit Kreditkarte oder mit PayPal. Bei PayPal wird mit dem Käuferschutz geworben.

Das Geld ist erst einmal weg und nun beginnt die Wartezeit. Und irgendwann kommt eventuell (es gibt Fälle da kam überhaupt nichts) ein Paket an. Der stolze Besitzer der DigiTennaMax macht sich an die Installation. Alle Kabel liegen



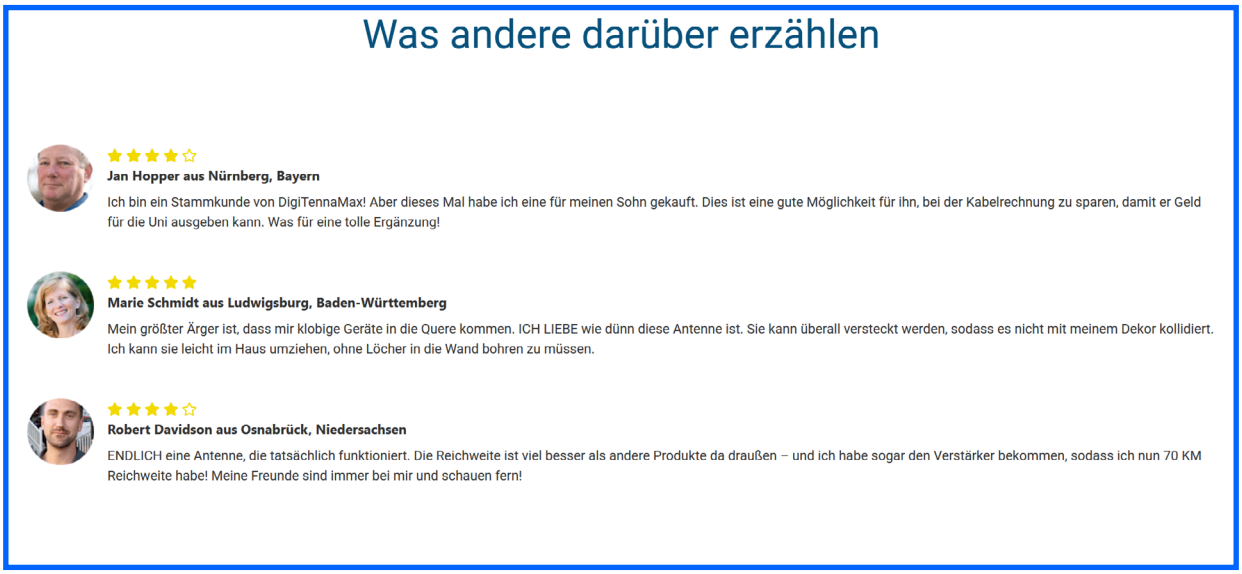
bei und die Passiv-Antenne entpuppt sich als Folienantenne für die Fensterscheibe. In Deutschland erhältlich für 8,99 Euro bei Amazon. Die Antenne ist passiv, das heißt, sie hat keinen integrierten Verstärker.

Unser Käufer hat zwar einen etwas älteren Flachbildschirm, jedoch keinen DVT T2 Tuner verbaut und einen externen Receiver hat er auch nicht. In der Werbung war davon keine Rede. Es hieß nur: Antenne am Fenster befestigen, Kabel anschließen und auf geht's. Resultat zu den 55 Euro für die Antenne kamen nochmals 30 Euro für den billigsten DVB T2-Receiver hinzu.

Einen Tag später war der Receiver da und der automatische Suchlauf wurde gestartet. Ganze vier Sender wurden eigelesen, doch das Signal war so schwach, dass Bild und Ton den Schwellenwert nicht überspringen konnten. Auch die Umplatzierung der Antenne brachte keinen Erfolg. Da blieb nur noch die zugesagte Rückgabe der Wunderantenne übrig. Es wurde eine Adresse für die Rückgabe in Bratislava angegeben.

Das Paket dorthin kostete noch einmal 16,50 Euro Porto. Bei PayPal wurde Konfliktlösung beantragt und daraus wurde ein „Case", der bis heute nicht gelöst wurde. Mails wegen der Rückerstattung des Kaufpreises beim Anbieter MDE Commerce Ltd. in Malta blieben unbeantwortet und nach vier Wochen kam das Paket als unzustellbar aus Bratislava zurück.

Und hier begann unsere Recherche.



Begonnen wurde mit den Rückgabestationen. Die Adressen wechseln immer wieder in sind zum Teil nicht existent. Es gab während unserer Recherche eine in Kleve, Deutschland, eine in den Niederlanden, eine in Estland und die aktuelle in Bratislava.

Hinter keiner dieser Anschriften gab es einen Ableger oder Beauftragten der MDE Commerce Ltd.

Die MDE Commerce Ltd. ist in Malta unter der Registernummer C86613 beim dortigen Handelsgericht eingetragen. Die Firma gibt selbst den Firmensitz mit 72, TRIQ TAL-QROQQ, MSIDA, Malta an. Das Haus ist ein kleineres Gebäude im Zentrum und beherbergt Briefkastenfirmen.

Eingetragen ist die Firma jedoch in der 1, Triq L Gherien und diese Villa wird durch den Geschäftsführer Ricardo Pereira bewohnt.

Offensichtlich lebt es sich ganz gut mit dem Handel von Wunderantennen. Bei näherer Untersuchung stellt sich heraus, dass die offizielle Telefonnummer +37256076645 in Estland beheimatet ist. Ruft man dort an, kommt eine Ansage, dass der gewünschte Teilnehmer z.Zt. nicht erreichbar sei. Ob Ricardo Pereira nur ein Strohmann ist, oder der Kopf hinter dem Unternehmen, bleibt erst einmal offen. Fest steht nach unseren Recherchen, dass MDE Commerce Ltd. mit dem Verkauf der DigiTennaMax wohl nur das Porto verdient.

MDE Commerce Ltd. „verkauft“ über einen Shop im Internet alles Mögliche. Vom Robotstaubsauger bis zum Luftreiniger. Nur die bestellten Waren kommen nicht an oder aber in den Paketen befindet sich wertloses Plastikmaterial. Auf der Seite der französischen Organisation „Signal-Arnaques“ findet man zahllose Berichte betroffener Menschen. Der Schaden dürfte in die Millionen gehen.

Fazit

Hände weg von Produkten der Firma MDE Commerce Ltd. und vor allen Dingen der DigiTennaMax oder wie si in Zukunft auch immer heißen mag.

8 digitale Technologien, die den Urlaub noch besser machen

Mehr Komfort durch Apps und smarte Hotels

Virtual und Augmented Reality ermöglichen neue Formen des Reisens

bitkom

Die Sommerferien haben begonnen und damit die Urlaubszeit. Eine Reise online oder per App zu buchen, ist dabei für viele schon selbstverständlich. Digitale Technologien könnten aber bald dafür sorgen, dass der Urlaub noch schöner und erholsamer wird – vorher, während der Reise und bei der Erinnerung daran.

Im Auftrag des Digitalverbands Bitkom wurden 1.004 Verbraucher ab 16 Jahren repräsentativ danach befragt, welche digitalen Innovationen sie für ihren Urlaub nutzen oder eher nutzen würden.

Dies sind die Ergebnisse:

1

Eine große Mehrheit will so nahtlos wie möglich reisen – also ohne lästige Pausen und Wartezeiten. Hat der Flug Verspätung, soll automatisch auch das Taxi zum Airport später kommen.
79 % der Befragten würden einen solchen Service nutzen.

2

Morgens ausschlafen – und zwar ohne dass plötzlich das Reinigungspersonal im Hotelzimmer steht: 69 % würden gern in einem smarten Hotel wohnen, das automatisch erkennt, ob der Gast sich gerade im Zimmer aufhält.

3

Sechs von zehn Reisenden (60 %) hätten Interesse an neuartigen Erlebniswelten durch Augmented Reality. Mithilfe von Smartphone-Apps werden zur besseren Orientierung und für Ausflugstipps digitale Inhalte zum realen Reiseort hinzugefügt.
Insbesondere jüngere Befragte zeigten sich daran interessiert:
72 % der 16- bis 29-Jährigen würden entsprechende Apps nutzen, bei den über 65-Jährigen sind es immerhin 44 %.

4

Mehr als jeder Zweite (55 %) würde gern vom Sofa aus mit einer Virtual-Reality-Brille auf Reisen gehen. Denkbar wäre, so schon vor dem Urlaub das Hotelzimmer zu besichtigen oder einen Blick in die Schluchten des Grand Canyon zu werfen. Aber auch eine Reise an noch unerreichbare Orte oder in vergangene Zeiten ist möglich.
Wie wäre es etwa mit einem Besuch auf dem Mars oder einem Gang durch das antike Rom?

5

Mithilfe von Fotos in Erinnerungen schwelgen ist schön. Dies mit 360-Grad-Bildern und einer VR-Brille zu tun, ist aber noch schöner. 54 % der Befragten würden sich ihre Urlaubsvideos nach der Rückkehr gern mit dieser Technologie anschauen.

6

39 % wünschen sich mehr Komfort durch ein smartes Hotel. Das Licht, die Raumtemperatur oder die Musik wollen sie entweder per Smartphone-App oder direkt per Sprachbefehl steuern.

7

Lange Wartezeiten an der Rezeption sind insbesondere nach einem langen Flug unschön. Jeder dritte Reisende (33 %) würde deshalb auch einen Service-Roboter nutzen, der ihn im Hotel empfängt und eincheckt. Vor allem jüngere Reisende zeigen sich hier aufgeschlossen: Jeder zweite 16- bis 29-Jährige (50 %) würde sich gern von einem Roboter im Hotel empfangen lassen. Bei den über 65-Jährigen ist es nur jeder Vierte (23 %).

8

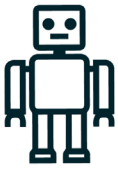
Wo habe ich nur die Keycard hingelegt...? Für 31 % soll das Suchen nach der Türkarte oder dem Zimmerschlüssel künftig der Vergangenheit angehören. Sie wollen ihr Smartphone als Türöffner nutzen und das Hotelzimmer künftig per App öffnen und wieder verschließen.

„*Die Digitalisierung verändert das Reisen derzeit von Grund auf. Statt nur in Reisekatalogen zu blättern, inspirieren und informieren wir uns online. Wir nutzen Social Media, Vergleichsportale und Blogs, suchen online nach Übernachtungen, Flügen und Fahrten, die zu unseren individuellen Wünschen passen. Doch das Potenzial ist damit längst noch nicht ausgeschöpft: Big Data, Virtual und Augmented Reality ermöglichen eine neue Form des Reisens, die den Urlaub nicht nur komfortabler, sondern auch spannender und informativer macht*“, sagt Bitkom-Hauptgeschäftsführer Bernhard Rohleder. „*Die Zahlen zeigen, dass viele Menschen diese Technologien nutzen würden. Es ist wichtig, dass alle touristischen Akteure sich mit den digitalen Innovationen auseinandersetzen, ihr Geschäftsmodell überprüfen und sich fit machen für den mobilen, vernetzten und smarten Tourismus der Zukunft. Die Digitalisierung ist für die gesamte Branche eine große Chance.*“

Hinweis zur Methodik: Grundlage der Angaben ist eine repräsentative Befragung, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.004 Verbraucher ab 16 Jahren in Deutschland telefonisch befragt. Die Fragestellungen lautete: „Welchen dieser Services würden Sie nutzen?“

Digitale Technologien auf Reisen

Welche dieser Services würden Sie nutzen?



Automatisierung

79% Wenn mein Flug Verspätung hat, wird automatisch das Taxi zum Flughafen später bestellt

69% Der Hotelservice erkennt automatisch, ob ich im Hotelzimmer bin

33% Im Hotel werde ich von einem Roboter empfangen

Smartphone-Apps

60% Augmented Reality mithilfe von Smartphone-Apps

39% Im Hotelzimmer kann das Licht, die Temperatur oder die Musik mithilfe einer App oder per Spracherkennung gesteuert werden

31% Ich kann mein Hotelzimmer mithilfe einer App per Smartphone öffnen und verschließen

Virtual Reality

55% Ich mache mit der VR-Brille virtuelle Reisen an existierende oder fiktive Orte

54% Ich schaue mir nach dem Urlaub mit einer VR-Brille 360-Grad-Urlaubsvideos an

Basis: 1004 Verbraucher ab 16 Jahren
Quelle: Bitkom Research

bitkom

Die Consumer Electronics-Trends der IFA 2019

Künstliche Intelligenz, mobile Geräte für die Zukunftsnetze in 5G, flexible Bildschirme, 360-Grad-Sound und drahtloses Musik-Streaming aus Vinylrillen

Als weltweit bedeutendste Messe für Consumer Electronics zeigt die IFA vom 06. bis zum 11. September 2019, wovon sich Millionen Kunden für ihre Einkäufe zur Weihnachtssaison inspirieren lassen – aber auch Innovationen, die weit über den Tageshorizont hinausweisen.

Künstliche Intelligenz, kurz KI, setzt in diesem Jahr spannende Trends: Viele Gerätearten arbeiten mit digitalen Systemen, die selbst lernen und damit im Lauf der Zeit immer leistungsfähiger werden. Sprachsteuerungssysteme zum Beispiel erweitern ihre Fähigkeiten kontinuierlich. Die jüngste Bildschirm-Generation mit 8kAuflösung braucht KI, um Bildinhalte mit den heute noch üblichen Auflösungen perfekt an das neue, extrem feine Pixelraster anzupassen. Und wenn es gilt, den Ton zum Bild optimal aufzubereiten, hilft KI ebenfalls: Intelligente Software erkennt, ob der Sound aus einem Fußballstadion, einem Nachrichtenstudio oder einem Konzertsaal kommt, und sorgt für entsprechende Feinjustage.

5G, die Technik für superschnelle Kommunikationsnetze der nächsten Generation, prägt weitere Neuheitentrends. So wird die IFA 2019 schon die ersten serienreifen 5G-Smartphones präsentieren, andere mobile Datengeräte werden rasch folgen.

Innovative Bildschirmtechniken setzen weitere spektakuläre IFA-Akzente – zum Beispiel flexible OLED-Displays: Großbild-Fernseher, die sich wie Rollos aufrollen und in kompakten Gehäusen verschwinden, werden die IFA-Besucher ebenso faszinieren wie Tablets, die sich auf die halbe Größe falten lassen, um sich so in handliche Smartphones zu verwandeln. Prototypen zeigen sogar schon, wie Mobiltelefone künftig aussehen könnten: wie breite Armreifen, die man sich dekorativ um das Handgelenk wickelt. Andere Bildschirm-Prototypen wechseln auf Befehl in einen transparenten Modus. Dann sehen sie aus wie Fensterscheiben – bis die Gerätesteuerung ihnen wieder bunte Bilder auf die Oberfläche schickt.

Micro LED, auch Crystal LED genannt, ist eine weitere Bildschirmtechnik mit Zukunftspotential. Solche Displays erzeugen die Bilder mit farbigen Pünktchen aus kristallinen Leuchtdioden – und inspirieren schon heute ganz neue Produktideen: Die IFA wird Micro LED-Schirme zeigen, die sich wie Kacheln zu beliebigen Formen und Größen kombinieren lassen.

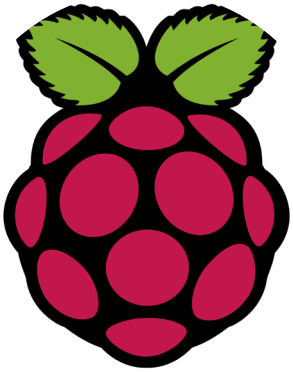
Für Bilder in wandfüllenden Größen sorgen neue Projektor-Generationen. Besonders wohnfreundliche Lösungen schaffen das aus kürzester Distanz – installiert in unmittelbarer Nähe der

Projektionsfläche. Andere interessante Modelle, die sich überall mühelos aufstellen lassen, stecken in schlanken, vertikalen Gehäusen mit Tragegriff. Sie werfen das Projektionslicht nach oben gegen aufklappbare Spiegel und positionieren die Bilder damit ohne komplizierte Einstell-Prozeduren passgenau auf der Leinwand. Spektakuläre Farben versprechen neue Projektoren, die als Lichtquellen separate Laserstrahlen in den Grundfarben Rot, Grün und Blau verwenden.

Für starken Ton zum großen Bild sorgt nicht nur ein breites Angebot an Soundbars, die mit der Wiedergabe von 3D-Tonformaten Heimkino-Atmosphäre erzeugen. Der jüngste Trend heißt 360-Grad-Wiedergabe: Rundum strahlende Lautsprecher, die auch die Höhendimension des Raums akustisch ausleuchten, verleihen dem Begriff Raumklang eine ganz neue Bedeutung.

Funklautsprecher zählen weiterhin zu den begehrtesten Gerätearten der Consumer Electronics. Viele Modelle lassen sich zu Multi-Room-Systemen vernetzen und sie alle wetteifern um die Gunst der Kunden mit einem immer größeren Musikangebot aus Streaming-Diensten – auch mit solchen, die Musik in hochauflösender Qualität über das Internet liefern.

Aber auch Vinylplattenspieler erfreuen sich anhaltender Beliebtheit. Die IFA spiegelt den Trend mit neuen Modellen, die Tonträger von gestern mit modernen HiFiKonzepten konfrontieren. Die jüngsten Geräte bestechen nicht nur mit feinmechanischer Präzision, sie bauen auch mit eingebauten Vorverstärkern und sogar mit integrierten Bluetooth-Sendern für den Musikfunk Brücken in die Moderne.



2

Raspberry Pi als VPN-Server einrichten

Tutorial mit OpenVPN

Die Sicherheit öffentlicher Internetzugänge lässt häufig zu wünschen übrig. Wenn Sie sich auch unterwegs sicher im Netz bewegen möchten, lässt sich dies gut über ein eigenes VPN („Virtual Private Network“ bzw. virtuelles privates Netzwerk) bewältigen. Wer sich einen persönlichen VPN-Server erstellt, hat außerdem über jede Internetverbindung Zugriff auf das heimische lokale Netzwerk.

Für die Einrichtung des eigenen virtuellen, privaten Netzwerks benötigt man einen Rechner, der als Server für dieses fungiert. Der Raspberry Pi stellt hierfür eine kostengünstige Option dar. Einen VPN-Server können Sie auf dem Raspberry Pi mit der freien VPN-Server-Software OpenVPN umsetzen, die als kostenfreier Download verfügbar ist.

Ein VPN richtet man in einem lokalen Netzwerk (LAN) ein, um auf dieses auch von außerhalb zugreifen zu können. Es stellt ein virtuelles Kommunikationsnetz dar, bei dem zumeist über das Internet die Anfragen und Antworten zwischen dem VPN-Server und den VPN-Clients (mit dem Server verknüpfte Geräte) transportiert werden.

Mit einem selbst eingerichteten VPN ist es somit möglich, von jedem beliebigen Internetzugang aus auf das eigene lokale Netzwerk zuzugreifen. Dadurch können Sie die im LAN befindlichen Daten zugreifen und einzelne Geräte aus der Ferne ansprechen (z. B. einen Drucker oder ein Faxgerät) sowie die Internetverbindung Ihres lokalen Netzwerks nutzen.

Dank einer verschlüsselten Verbindung zu Ihrem VPN-Server können Sie sich zudem weitaus sicherer im Netz bewegen, als wenn Sie auf risikobehaftete, offen zugängliche Internetanschlüsse (wie öffentliche WLANs) zurückgreifen würden.

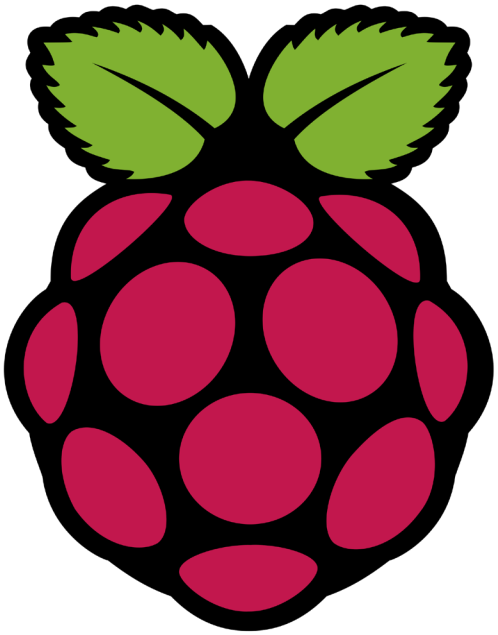
Damit eine solch sichere Verbindung zu einem VPN-Server möglich ist, müssen Sie allerdings in Ihrem lokalen Netzwerk auf einem Rechner einen VPN-Server einrichten, der ständig mit dem Internet verbunden ist. Der Computer fungiert dann als Host für das virtuelle private Netzwerk. Über eine Client-Software verbinden Sie Geräte (wie Laptop, Smartphone oder Tablet) mit dem Server. Wenn Sie nun mit einem Client über eine Internetverbindung, die außerhalb Ihres persönlichen LANs liegt, auf Ihren VPN-Server zugreifen, geschieht dies über eine verschlüsselte Verbindung (VPN-Tunnel genannt).

Dieser VPN-Tunnel beginnt bei Ihrem Client und endet bei Ihrem VPN-Server – er erstreckt sich durch die komplette Internetverbindung. Dabei ist der Tunnel um ein Vielfaches sicherer als durchschnittliche öffentliche Internetverbindungen. Hacker haben es dementsprechend schwer, in den Tunnel einzudringen und den Datenverkehr mitzuschneiden.

Über eine persönliche VPN-Verbindung können Sie deshalb auch in öffentlichen WLANs sehr sicher mit sensiblen Daten arbeiten (wie z. B. beim Online-Banking).

VPN-Server erstellen mit dem Raspberry Pi und OpenVPN: Die Vorteile

Die geringen Kosten für einen Raspberry Pi machen ihn als VPN-Server so attraktiv. Der Einkaufspreis des kleinen Computers und des nötigen Zubehörs ist vergleichsweise niedrig. Darüber hinaus ist auch sein Stromverbrauch für den dauerhaften Betrieb eines Servers auf dem Rechner relativ gering. Generell bietet er ein gutes Preis-Leistungs-Verhältnis (auch wenn inzwischen verschiedene Raspberry-Pi-Alternativen existieren).



OpenVPN eignet sich für ein VPN aus mehreren Gründen: Es handelt sich dabei um ein kostenfreie, weit verbreitete VPN-Server-Software, die eine große Anzahl an Betriebssystemen unterstützt (Windows, OS X, Android, iOS, Linux und weitere). Außerdem überzeugt das Programm mit einer vergleichsweise einfachen Einrichtung und einer hohen Stabilität.

Was benötigt man für die Einrichtung eines VPN-Servers auf dem Raspberry Pi?

Für das nachstehende Tutorial benötigen Sie Folgendes:

- *Raspberry Pi (empfohlen: Modell 2 oder höher)*
- *Micro-SD-Speicherkarte mit installiertem Raspbian-Jessie-Betriebssystem*
- *Kontinuierlich vorhandene Internetverbindung (am besten per Netzwerkkabel) und Stromversorgung (Micro-USB-Kabel) für den Raspberry Pi.*

Darüber hinaus müssen Sie entscheiden, ob Sie direkt am Raspberry Pi den VPN-Server einrichten möchten (mit angeschlossenem Monitor und verbundener Maus und Tastatur) oder aber über einen SSH-Client.

Die Fernwartung des Servers mittels SSH ist in den meisten Fällen die empfehlenswertere Variante, da Sie hierüber am einfachsten von einem

anderen Rechner aus auf den späteren VPN-Server zugreifen können.

Zu diesem Zweck gibt es verschiedene weit verbreitete Software wie PuTTY, WinSCP oder OpenSSH (für Unix-Betriebssysteme), über die Sie den Raspberry Pi ansteuern und bedienen können. Sie verbinden die SSH-Software mit dem Raspberry Pi, indem Sie dessen IPv4-Adresse in dem Client (den Rechner, mit dem Sie auf den Raspberry Pi zugreifen möchten) angeben und beide miteinander verknüpfen.

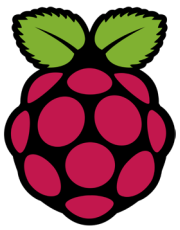
Die IP-Adresse Ihres Raspberry Pis können Sie sich beispielsweise über das Router-Menü im Browser anzeigen lassen. Sie gelangen in der Regel dorthin, wenn Sie die Adresse „192.168.0.1“ (bzw. bei Fritz!Box-Besitzern „fritz.box“) in Ihrem Browser aufrufen.

IP-Adressen anpassen

Für die Nutzung eines SSH-Clients ist es ratsam, dem Raspberry Pi eine statische private IP-Adresse im lokalen Netzwerk zuzuordnen – andernfalls müssen Sie jeden Tag, an dem Sie via SSH auf den Mini-Computer zugreifen möchten, aufs Neue seine momentane dynamische Adresse heraussuchen und den Client mit dieser verbinden. Noch wichtiger ist die Verknüpfung einer beständigen privaten IP-Adresse mit dem Raspberry Pi für die Nutzung von OpenVPN: Der VPN-Server muss im lokalen Netzwerk permanent unter derselben Adresse erreichbar sein, damit Sie kontinuierlich auf ihn zugreifen können.

Darüber hinaus sollten Sie den VPN-Server auch permanent unter derselben Adresse über das Internet erreichbar halten. Für gewöhnlich verfügt ein Internetanschluss jedoch nur über eine dynamische öffentliche IP-Adresse, die spätestens nach 24 Stunden wechselt und so die ständige Erreichbarkeit des Servers unter derselben IP-Adresse vereitelt. Falls Ihre Internet-verbindung über keine statische öffentliche IP-Adresse verfügt, können Sie sich aber mit der Einrichtung eines dynamischen DNS (DDNS) behelfen.

In einem anderen Artikel können Sie nachlesen, wie Sie dem Raspberry Pi eine statische IP-Adresse zuordnen und welche Möglichkeiten es für die Einrichtung von DDNS gibt. Wenn Sie Ihren Raspberry Pi als Server permanent online verfügbar halten möchten, sollten Sie sich regelmäßig um seine Aktualisierung und Sicherheit kümmern.



Mit OpenVPN einen eigenen VPN-Server auf dem Raspberry Pi installieren

Nun kann die Einrichtung von OpenVPN beginnen. Zu diesem Zweck öffnen Sie das Terminal (die Eingabe-Konsole) Ihres Raspberry Pis.

Vorbereitung des Raspberry Pis

Bevor Sie sich der Installation von OpenVPN zuwenden, empfiehlt es sich, für die bereits vorhandenen Pakete auf dem Raspberry Pi nach Updates zu suchen und diese zu installieren. Geben Sie hierfür folgende Kommandos in die Konsole ein:

sudo apt-get update

sudo apt-get upgrade

Falls Sie das voreingestellte Standardpasswort Ihres Raspberry Pis (Benutzername: „Pi"; Passwort: „Raspberry") noch nicht geändert haben, sollten Sie dies nun dringend nachholen: Andernfalls kann sich jeder Zugang zum System verschaffen – sowohl lokal als auch über das Netzwerk via SSH. Mit dem unten stehenden Befehl rufen Sie die Konfiguration des Mini-Rechners auf, in der Sie ein sicheres Kennwort anlegen können.

sudo raspi-config

OpenVPN installieren und easy-rsa-Datei einrichten

Zunächst installieren Sie über den folgenden Befehl die OpenVPN-Software sowie OpenSSL, das der Verschlüsselung der Internetverbindung dient.

sudo apt-get install openvpn openssl

Nach der Installation von OpenVPN kopieren Sie die vorgefertigten Skripte **„easy-rsa"** in das OpenVPN-Konfigurationsverzeichnis. Hierüber legen Sie verschiedene Zertifikate und Schlüssel an. Das folgende Kommando funktioniert nur unter Raspbian Jessie (beim Vorläufer-Betriebssystem Wheezy liegen die Skripte unter „/sr/share/doc/openvpn/examples/easy-rsa/2.0").

sudo cp -r /usr/share/easy-rsa /etc/openvpn/easy-rsa

Öffnen Sie als Nächstes in der Konsole die Datei „/etc/openvpn/easy-rsa/vars", indem Sie folgenden Befehl ausführen:

sudo nano /etc/openvpn/easy-rsa/vars

Jetzt gilt es, diese Datei anzupassen. Sie ändern die Einstellungen, indem Sie die komplette Zeile **„export EASY_RSA="`pwd`""** durch die Folgende ersetzen:

export EASY_RSA="/etc/openvpn/easy-rsa"

Die Schlüssellänge lässt sich in der Datei ebenfalls anpassen, wodurch Sie das Sicherheitsniveau der Verschlüsselung festlegen. Ein Raspberry Pi 3 verfügt über genügend Rechenleistung, um ohne Probleme eine Schlüssellänge von 2048 Bit verarbeiten zu können.

Bei dem Modell 2 führt diese Verschlüsselung jedoch schon zu merklichen Performance-Einbußen, sodass Sie in diesem Fall eventuell nur eine 1024-Bit-Verschlüsselung verwenden sollten – je nachdem, ob Ihnen die Geschwindigkeit oder die Verschlüsselung der Verbindung wichtiger ist.

Eine 4096-Bit-Verschlüsselung ist hingegen nur in den wenigsten Fällen sinnvoll. Sie ändern die Schlüssellänge durch die Anpassung der Bit-Zahl in der Zeile **„export KEY_SIZE=2048“**

Nun gehen Sie zurück in das Konfigurationsverzeichnis **„easy-rsa“**, geben sich Root-Rechte und integrieren dann die vorher getätigten Einstellungen in die Umgebungsvariablen, indem Sie das Skript **„vars“** mit dem Befehl **„source“** ausführen. Anschließend machen Sie die entstehende Konfigurationsdatei über einen symbolischen Link unter dem Namen **„openssl.cnf“** zugänglich.

```
cd /etc/openvpn/easy-rsa

sudo su

source vars

ln -s openssl-1.0.0.cnf openssl.cnf
```

Zertifikate und Schlüssel für OpenVPN erstellen

Zunächst setzen Sie die Schlüssel zurück und erstellen dann die ersten Schlüsseldateien für OpenVPN.

```
./clean-all

./build-ca OpenVPN
```

Sie werden aufgefordert, den zwei Buchstaben umfassenden „Country Name“ Ihres Landes einzutragen (DE für Deutschland, AT für Österreich und CH für die Schweiz). Die anschließenden Abfragen sind nicht weiter von Belang und Sie können sie einfach ohne Angaben mit der Eingabetaste bestätigen.

Anschließend generieren Sie die Schlüsseldateien für den Server:

```
./build-key-server server
```

Geben Sie ein weiteres Mal den zweistelligen Länder-Code ein und belassen die darauffolgenden Felder leer. Abschließend bestätigen Sie die Anfrage, ob das Zertifikat generiert werden soll, zwei Mal mit „Y“.

Nachfolgend widmen Sie sich der Einrichtung eines oder mehrerer VPN-Clients. Dabei erstellen Sie für jedes Gerät, mit dem

Sie auf den VPN-Server zugreifen möchten, ein Zertifikat und einen Schlüssel.

Der Ablauf ähnelt dabei dem bei der Einrichtung von Zertifikat und Schlüssel beim Server (Länderkürzel eintragen und zwei Mal bestätigen). Sie können jedem der Geräte einen spezifischen Namen zuweisen (im unten stehenden Befehl wird je ein Client für ein „laptop“, „smartphone“ und ein „tablet“ angelegt).

./build-key laptop

./build-key smartphone

./build-key tablet

...

Wenn Sie die Clients mit einem Passwort versehen möchten, nutzen Sie statt der oben stehenden Befehle die Folgenden:

./build-key-pass laptop

./build-key-pass smartphone

./build-key-pass tablet

...

Die Erzeugung der Zertifikate und Schlüssel schließen Sie mit dem Befehl für den Diffie-Hellman-Schlüsselaustausch ab:

./build-dh

Dies kann unter Umständen etwas mehr Zeit in Anspruch nehmen. Sobald der Vorgang abgeschlossen ist, melden Sie sich als Root-Benutzer ab:

exit

Konfigurationsdatei für OpenVPN-Server generieren

Rufen Sie die OpenVPN-Konfigurationsdatei auf:

sudo nano /etc/openvpn/openvpn.conf

Die leere Datei füllen Sie nun mit diversen Befehlen, die wir im Folgenden erläutern. Zunächst aktivieren Sie über „dev tun“ das Routing durch einen IP-Tunnel und wählen mit „proto udp“ UDP als Transportprotokoll aus (falls Sie TCP verwenden möchten, wählen Sie „proto tcp“). In der darauffolgenden Zeile legen Sie fest, dass der OpenVPN-Server auf dem Port 1194 erreichbar ist – Sie können diesen aber auch ändern.

dev tun

proto udp

port 1194

Als Nächstes erstellen Sie ein SSL/TLS Root-Zertifikat (ca), ein digitales Zertifikat (cert) und einen digitalen Schlüssel (key) über das Verzeichnis „easy-rsa“. Des Weiteren sollten Sie darauf achten, dass Sie die richtige Bit-Verschlüsselung eintragen (1024, 2048 etc.).

ca /etc/openvpn/easy-rsa/keys/ca.crt

cert /etc/openvpn/easy-rsa/keys/server.crt

key /etc/openvpn/easy-rsa/keys/server.key

dh /etc/openvpn/easy-rsa/keys/dh2048.pem

Nun legen Sie fest, dass der Raspberry Pi als VPN-Server genutzt wird. Hierfür nennen Sie IP-Adresse sowie die Netzmaske, die dem VPN zugeordnet werden soll.

server 10.8.0.0 255.255.255.0

Mit dem Kommando „**redirect-gateway def1 bypass-dhcp**" leiten Sie nun den kompletten IP-Traffic durch den IP-Tunnel. Wenn Sie hohe Sicherheitsanforderungen haben, können Sie mit dieser Einstellung experimentieren – falls sich dadurch Schwierigkeiten ergeben oder das Surfen zu langsam wird, ist es jedoch ratsam, diese Konfiguration wieder abzustellen.

Die anderen unten aufgelisteten Anweisungen sollten Sie hingegen in jedem Fall verwenden: Über sie benennen Sie die öffentlichen DNS-Server, mit denen Ihr VPN-Server arbeiten wird.

Im nachstehenden Befehl ist mit „**217.237.150.188**" ein Server von 1&1 IONOS sowie mit „**8.8.8.8**" einer von Google gelistet. Diese können Sie aber durch die Angabe der IPv4-Adressen anderer DNS-Server nach Belieben austauschen. Über „**log-append /var/log/openvpn**" stellen Sie dann noch ein, dass die Log-Information in die Datei „**/var/log/openvpn**" geschrieben wird.

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 217.237.150.188"

push "dhcp-option DNS 8.8.8.8"

log-append /var/log/openvpn

Via „**persist-key**" werden Key-Dateien nicht erneut gelesen und mit „**persist-tun**" die TUN- und TAP-Netzwerk-Treiber nicht neu gestartet. Die Rechte des OpenVPN-Daemons nach einem Programmstart setzen Sie über „**user nobody**" und „**group nogroup**" herab. Mit „**status /var/log/openvpn-status.log**" erstellen Sie eine Status-Datei, die Ihnen die gegenwärtige Verbindung anzeigt.

Weiterhin ist es ratsam, die Ausführlichkeit der Log-Informationen mithilfe des Befehls „**verb**" zu vereinbaren. Wenn Sie dabei „**0**" wählen, erhalten Sie – abgesehen von Fehlermeldungen – keine Ausgaben. Ein Wert zwischen 1 und 4 eignet sich für den normalen Gebrauch, wohingegen sich darüber liegende Werte für die Fehlerbehebung eignen. Zuletzt bestimmen Sie noch über das Kommando „**client-to-client**", dass VPN-Clients nicht nur den Server, sondern auch andere VPN-Clients erkennen, und aktivieren mit „**comp-lzo**" die LZO-Komprimierung (diese müssen Sie auch in der config-Datei des Clients freigeben).

persist-key

persist-tun

user nobody

group nogroup

status /var/log/openvpn-status.log

verb 3

client-to-client

comp-lzo

Mit "Strg + O" speichern Sie die Änderungen und mit „Strg + X" beenden Sie den Editor.

Skript für den Internetzugriff mit einem Client anlegen

Damit Sie über Ihren VPN-Tunnel auf den Internetanschluss Ihres lokalen Netzwerks zugreifen können, müssen Sie eine Weiterleitung erstellen. Legen Sie hierfür zunächst die Datei „**/etc/init.d/rpivpn**" an:

Sudo nano /etc/init.d/rpivpn

Indem Sie die folgenden Kommentare in die Datei kopieren, erstellen Sie den Header für ein Linux-Init-Skript:

#! /bin/sh

BEGIN INIT INFO

 # Provides: rpivpn

 # Required-Start: $remote_fs $syslog

 # Required-Stop: $remote_fs $syslog

 # Default-Start: 2 3 4 5

 # Default-Stop: 0 1 6

 # Short-Description: VPN initialization script

END INIT INFO

Nachfolgend aktivieren Sie „**ip_forward**", indem Sie eine „**1**" in diese Datei schreiben:

echo 'echo "1" > /proc/sys/net/ipv4/ip_forward' | sudo -s

Als Nächstes legen Sie über den Paketfilter „**iptables**" eine Weiterleitung für VPN-Pakete an.

iptables -A INPUT -i tun+ -j ACCEPT

iptables -A FORWARD -i tun+ -j ACCEPT

Es sind nun noch Befehle erforderlich, die Ihren VPN-Clients den Zugang zum LAN und zum Internet gewähren. Diese richten Sie mit den folgenden Zeilen ein:

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -t nat -F POSTROUTING

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

Speichern und schließen Sie die Datei erneut mit „Strg + O" und „Strg + X".

Damit die Weiterleitung funktioniert, müssen Sie dem Skript noch die entsprechenden Rechte zuteilen und es als Init-Skript installieren.

sudo chmod +x /etc/init.d/rpivpn

sudo update-rc.d rpivpn defaults

Nun führen Sie das Skript aus und starten danach den OpenVPN-Server neu.

sudo /etc/init.d/rpivpn

sudo /etc/init.d/openvpn restart

Einrichtung der Clients abschließen

Im letzten Schritt bündeln Sie die Zertifikate und Schlüssel jedes Clients in einem eigenen Paket. Hierfür geben Sie sich wieder Root-Rechte, öffnen den Ordner „/etc/openvpn/easy-rsa/keys/“ und legen die Client-Konfigurationsdatei an. Über die folgenden Befehle rufen Sie die Datei des „laptop“-Clients auf. Die Einrichtung jedes Clients funktioniert immer gleich – Sie müssen lediglich die Bezeichnung des Geräts entsprechend abändern.

sudo su

cd /etc/openvpn/easy-rsa/keys

nano laptop.ovpn

In der „.ovpn“-Datei des Clients fügen Sie nun Folgendes ein:

dev tun

client

proto udp

remote x.x.x.x 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert laptop.crt

key laptop.key

comp-lzo

verb 3

Den oben stehenden Dateiinhalt müssen Sie allerdings noch anpassen. In der vierten Zeile ersetzen Sie „x.x.x.x“ mit der IP-Adresse Ihres DDNS-Anbieters (falls Sie eine statische öffentliche IP-Adresse nutzen, können Sie selbstverständlich einfach diese dort eintragen), gefolgt von dem Port, über den der VPN-Server erreichbar sein soll. In der dritt- und viertletzten Zeile tragen Sie den Namen Ihres Clients ein (hier: „laptop“).

Nachdem Sie die Änderungen vorgenommen haben, speichern Sie diese mit „Strg + O“ und schließen den Editor mit „Strg + X“.

Als Letztes fügen Sie die Konfigurationsdatei mit ihren Zertifikaten und Schlüsseln in einer Zip-Datei zusammen. Falls Sie noch kein Zip-Paket auf dem Raspberry Pi installiert haben, gelingt dies beispielsweise mit folgendem Befehl:

apt-get install zip

Zum Erstellen der Zip-Datei nutzen Sie die folgenden Befehle und achten dabei wieder darauf, dass Sie überall den richtigen Client-Namen einsetzen.

zip /home/pi/raspberry_laptop.zip ca.crt laptop.crt laptop.key laptop.ovpn

Nun müssen Sie noch die Rechte der Dateien anpassen und beenden danach die Einrichtung mit „exit“.

chown pi:pi /home/pi/raspberry_laptop.zip

exit

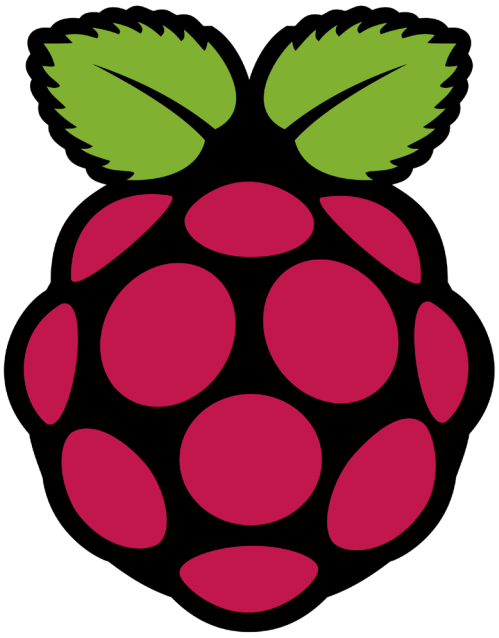
Die nun fertige Zip-Datei übertragen Sie vom Raspberry Pi auf den Client (beispielsweise über ein SCP- oder SFTP-Programm) und richten dann auf dem Gerät den Client ein. Nun können Sie mit dem Gerät von jedem beliebigen Internetanschluss aus auf das mit dem Client verbundene lokale Netzwerk und dessen Internetanschluss zugreifen.

Auf dem Raspberry Pi den eigenen VPN-Server einrichten lohnt sich

Das eigene VPN ist weit weniger kostspielig, als viele denken: Dank des geringen Stromverbrauchs des Raspberry Pis fallen keine großen laufenden Kosten an. Und auch die Ausgabe für die einzelnen Komponenten des Servers (Raspberry Pi, Micro-SD-Karte, usw.) sind überschaubar.

Zudem ist ein Raspberry-Pi-VPN-Server zu vielem imstande. Denn mit Ihrem selbstgehosteten VPN-Server auf dem Raspberry Pi können Sie von jeder Internetverbindung aus auf Ihr lokales Rechnernetzwerk zugreifen. Dabei ist die VPN-Verbindung verschlüsselt und ermöglicht es Ihnen, sich sowohl in einem offenen und/oder nicht vertrauenswürdigen WLAN als auch über die Datenleitung Ihres Mobilfunkvertrags deutlich sicherer im Netz zu bewegen. Viel mehr Schutz kann eine mobile Internetverbindung kaum bieten.

Diese Serie entstand mit der freundlichen Unterstützung durch den 1&1 IONOS Digital Guide.



Hörfunkverbreitung über 5G-Netze

5G-Media Initiative nimmt Stellung dazu

Die 5G Media Initiative wurde von namhaften Firmen und Organisationen ins Leben gerufen, um das Potential des zukünftigen Netzstandards 5G für die Medienbranche mit Forschung und Entwicklung zu fördern. Zu den Partnern gehören die Bayerische Landeszentrale für neue Medien, der Bayerische Rundfunk, das Münchner Start-up-Unternehmen Cadami, das Fraunhofer-Institut für Integrierte Schaltungen IIS, die Friedrich-Alexander-Universität Erlangen-Nürnberg FAU, das Institut für Nachrichtentechnik der TU Braunschweig, das Institut für Rundfunktechnik IRT, Kathrein SE, Media Broadcast GmbH, MUGLER, Nokia, Rohde & Schwarz, der Südwestrundfunk und Telefónica.

Die 5G Media Initiative vernetzt Medien, Wissenschaft und Industrie, um Know-How auszutauschen, gemeinsame Positionen zu erarbeiten und Forschungsprojekte zu initiieren.

Vor dem Hintergrund der Diskussion um die Hörfunkverbreitung mit 5G gilt es zwischen 5G-Mobilfunk im Unicast-Modus und einem 5G-Broadcast-Modus zu unterscheiden.

5G-Mobilfunk

5G wird im Laufe der kommenden Jahre als reines Mobilfunksystem (Unicast, Punkt-zu-Punkt Verbindungen) in den Markt kommen. Für die technischen Möglichkeiten einer Hörfunkverbreitung (Audiostreams) ergeben sich damit nur marginale Unterschiede zum existierenden 4G-Mobilfunk (LTE).

5G wird sich als von Mobilfunkbetreibern bereitgestellte Technik an deren wirtschaftlichen Rahmenbedingungen ausrichten. Eine 5G-Flächendeckung im Unicast-Modus, welche mit Rundfunksystemen annähernd vergleichbar wäre, ist derzeit nicht absehbar.

Die Unicast-Verbreitung von Hörfunk via Audiostreaming im Mobilfunksystem ist technisch betrachtet seit vielen Jahren möglich.

5G-Broadcast

Der europäische Rundfunk engagiert sich seit Jahren, den 5G-Standard so zu erweitern, dass die Verbreitung von linearen TV-Programmen zukünftig möglich sein wird. Dazu können existierende Rundfunksendeanlagen (High Tower High Power) verwendet werden, von denen ähnlich wie bei DVB-T2 ein Signal von einem Sender gleichzeitig an eine unbegrenzte Anzahl von Empfängern gesendet wird. Dies erlaubt einen unabhängigen Netzbetrieb durch Rundfunknetzbetreiber.

Diese Erweiterungen des globalen 5G-Standards werden unter dem Titel „5G Broadcast“ öffentlich diskutiert, technisch handelt es sich um FeMBMS (Further evolved Multimedia Broadcast Multicast Service).

Die Standarderweiterung und die geplanten Versorgungsstrukturen orientieren sich an den Erfordernissen einer TV-Verbreitung. Das primäre Ziel dabei ist es, free-to-air-TV-Angebote auf Endgeräte wie Smartphones, Tablets und in Fahrzeuge zu bringen. Die Verbreitung von linearen TV-Programmen zur umfangreichen, parallelen Nutzung profitiert aufgrund der hohen Datenraten von einem Rundfunkmodus.

Ohne Zweifel kann 5G-Broadcast aus technischer Sicht auch für die Verbreitung von linearen Hörfunkprogrammen verwendet werden. Die speziellen Anforderungen des Hörfunks an die Verbreitung seiner linearen Inhalte, wie z.B. flächendeckende Versorgung und Regionalisierung, werden durch die Einführung von 5G-Broadcast nicht automatisch erfüllt. Die derzeitigen Versorgungsziele richten sich an den Vorgaben für TV aus.

Der Hörfunkmarkt allein besitzt nicht genügend wirtschaftliches Potential, um die Marktdurchdringung von 5G-Broadcast voranzutreiben. Erst wenn der 5G-Broadcast-Markt für TV angelaufen ist, ergeben sich theoretisch Optionen für den Hörfunk. In der Konsequenz bedeutet dies, dass auch ein Markterfolg von 5G-Broadcast für TV nicht automatisch eine erfolgreiche Nutzungsmöglichkeit für Hörfunk bedeutet.

Eine erfolgreiche Markteinführung von 5G-Broadcast für TV muss noch einige Hürden überwinden. An erster Stelle steht die Verfügbarkeit von Chipsets und Endgeräten, die 5G-Broadcast unterstützen, sowie von ausreichendem Spektrum. Die 5G Media Initiative arbeitet branchenübergreifend an diesen Themen, um 5G-Broadcast voranzutreiben.

MEDIEN

Gefährliche Apps in Mediaplayern

Gerd. H aus Brandenburg ist wie die meisten Menschen ein Laie oder einfach nur faul, wenn es um die Installation von Apps in einem Mediaplayer geht. Einschalten und alles muss da sein, das ist seine Devise. Und da kam die Werbung für den Mediaplayer „MXQ Pro Android TV Box - Fully Loaded" gerade recht. Kodi und Mobdro waren an Bord und so stand dem kostenlosen Genuss von Spielfilmen und Pay-TV nichts mehr im Wege.

40 Euro gingen per Paypal an den Anbieter und vier Tage später war er stolzer Besitzer der kleinen Box. Und weil das so günstig war, abonnierte er auch noch gleich Netflix dazu.

Gerd H. war glücklich.

Allerdings gab es nach ein paar Wochen ab und zu Probleme mit Netflix. Der Streamingdienst verweigerte den Zutritt mit dem Hinweis, er sei bereits eingeloggt. Als dann in der Liste der kürzlich angesehenen Filme Titel zu sehen waren, die ihm völlig unbekannt waren, hätte er wach werden müssen.

Das wurde er erst, als von seinem Paypal Konto (Benutzername und Passwort waren identisch den Daten für Netflix) das gesamte Plus von 835,- Euro an einen Empfänger in Asien abwanderte.

Ein Einzelfall? Mitnichten! Der Umsatzzahlen bei den Mediaplayern steigen in Europa rasant an, doch liegt die Nutzung noch weit hinter der der Amerikaner. 75% der Amerikaner be-richten, dass sie mindestens mehrmals im Monat Unterhaltung streamen.
Das meiste davon geschieht über seriöse und bekannte Dienste wie Netflix, Amazon Prime Video und Hulu. In weniger als einem Jahrzehnt haben rund 250 Millionen Kunden weltweit diese Dienste in Anspruch genommen. Und diese Zahl wird sprunghaft ansteigen, wenn andere große Medienunternehmen in den kommenden Monaten ihre eigenen Streamingdienste einführen. Während kein Service absolut narrensicher ist, haben die Verbraucher bei bekannten Marken berechtigte Erwartungen an die Sicherheit.

Einige Verbraucher unternehmen jedoch riskante Schritte, um außerhalb der Mainstream-App-Marktplätze shoppen zu gehen, um ihre Wunschinhalte zu finden. Wenn Sie sich die Studentenwohnheime, die Männerhöhle eines Freundes oder das Schlafzimmer eines Teenagers ansehen, können Sie diesen Unterbau des Streamings finden: Pirateriegeräte wie Jailbreak Amazon Fire TV-Stick oder eine

sogenannte Kodi-Box, die alle mit illegalen Apps betrieben werden.

In einigen Fällen handelt es sich bei diesen Endgeräten um Set-Top-Boxen - oft aus China importiert - mit wenig vorinstallierter Software, die die Geräteverkäufer mit "Kodi" und Apps aufladen, die auf das Piraterie-Ecosystem zugreifen. In anderen Fällen werden legitime Geräte mit einer Software geladen, die den Zugriff auf illegale Apps ebenso einfach macht, wie auf legitime Apps wie Netflix oder Hulu. Nach dem Laden der Geräte mit den illegalen Apps (einige davon sind kostenlos und andere erfordern eine Abonnementgebühr) werden die Geräte gegen einen erheblichen Aufschlag an die Verbraucher verkauft - oft unter dem Motto: "Zahle niemals mehr für PayTV".

Die Geräte werden hauptsächlich für einen Zweck verwendet: den illegalen Zugriff auf raubkopierte Filme, Fernsehsendungen, Spiele und Musik. In einigen Fällen werden sie verwendet, um Zugang zu Filmen zu erhalten, die sich noch im Kino befinden. Pirateriegeräte stellen nicht nur eine Bedrohung für das legitime Content-Ecosystem dar, sondern auch für die Cybersicherheit insgesamt. Da Millionen von Geräten - von Telefonen, Tablets und Unterhaltungsgeräten bis hin zu Smart TVs, Thermostaten und Türklingeln - in das Haus gelangen, ist die Fähigkeit von Hackern, ein Haus über diese Boxen zu infiltrieren, unproblematisch.

Der Grund dafür, dass Kodi-Boxen besonders anfällig für Hacking sind, ist zweifach. Zuerst umgehen die Boxen die Sicherheitsmaßnahmen, die im Router enthalten sind. Zweitens sind bei der Konfiguration dieser Boxen normale Sicherheitsvorkehrungen in der Regel nicht installiert oder deaktiviert, um Anwendungen für das Streaming von illegalen Inhalten zu unterstützen. Für Android-Nutzer öffnet die Deaktivierung von Sicherheitsfunktionen beispielsweise einen bestimmten Port, auf dem Botnets routinemäßig scannen.

Einmal erkannt, greift der Hacker gezielt auf dieses Gerät, um es zu infizieren. Darüber hinaus müssen Benutzer, um die Apps nutzen zu können, der App oft vollen Administratorzugriff gewähren, der die Berechtigung zum Zugriff auf den gesamten Speicher des Geräts, sowie dessen Standort und andere Sicherheitsvorkehrungen beinhaltet. Nachdem die XMBC Foundation, die Kodi entwickelte, zunächst Beschwerden darüber ignoriert hatte,

wie sehr Kodi anfällig für Piraterie ist, verurteilte sie Piraten-Addons, weil sie Kodi einen schlechten Ruf einbringen. Das war es dann aber auch schon. Der Löwe hat mal kurz gebrüllt.

Angesichts der zunehmenden Bedenken haben Digital Citizens (*1) und Dark Wolfe (*2) eine Untersuchung eingeleitet. Um das Ecosystem der Streaming-Piraterie zu erforschen,
haben die Forscher von Dark Wolfe sechs Streaming-Geräte erworben, die die Kodi-Plattform nutzen. Die Quellen der Einkäufe waren unterschiedlich:

Online-Käufe von Websites, die bei der Suche über Google, Bing und Dogpile gefunden wurden und der Direktkauf bei einem lokalen Händler. Diese Geräte werden typischerweise als "vorinstalliert" mit Apps vermarktet, die es dem Benutzer ermöglichen, kostenlos oder gegen eine geringe monatliche Abo-Gebühr auf On-Demand-Filme (auch solche, die sich noch im Kinostart befinden) und Fernsehprogramme, sowie Live-Echtzeitübertragungen und Kabelunterhaltung, Sport- und Nachrichtenkanäle aus aller Welt zuzugreifen. Die illegalen Apps wiederum werden oft in App-Repositories gesammelt, die als "Repos" bezeichnet werden, in denen der Benutzer dann die gewünschten Apps herunterladen kann.

Mediaplayer mit illegalen Apps werden aus Sicherheitsgründen oft auf Dark Web Marktplätzen beworben. Verkäufer bieten Geräte wie den "MXQ Pro fully loaded" an, die mit einem kompletten

Satz von Kodi-Builds versehen sind und in den meisten Ländern als illegal gelten.

„Dream Market“ und "rstforums", etablierte Untergrundmärkte, bieten haufenweise illegale Mediaplayer an. „Dream Market“ ist ein Dark Net Marktplatz im Internet, auf dem eine Vielzahl illegaler Produkte zum Verkauf stehen - darunter Medikamente, Falschgeld, Waffen und gefälschte Kreditkarten.

Ein weiterer Bestandteil der Piraterie gestützten Ecosysteme ist die Werbung. Wie „Digital Citizens“ bei Piraterie-Websites festgestellt hat, integrieren illegale Akteure Mainstream-Werbung (z.B. Mini Cooper) in ihre Angebote. Damit schaffen sie eine potenzielle neue Einnahmequelle und erwecken den Eindruck von Seriosität.

Die Forscher von Dark Wolfe stellten fest, dass einige Piraterieverfechter zwar die "Vorteile" kostenloser Inhalte propagieren - UFC-Kämpfe, Live-Sportveranstaltungen, mehr Filme -, aber die Nutzer nicht vor der potenziellen Bedrohung durch Malware warnen. Das ist beunruhigend, da diese Software bei den Hackern beliebt ist, weil sie es ihnen ermöglicht, Malware recht unkompliziert über den Inhalt zu verbreiten.

Filme, Geld und Malware: Wie die Piraten Unternehmen und Verbraucher angreifen

Die Enthüllung, dass Kriminelle die Mediaplayer ins Visier nehmen, um Malware zu installieren, ist ein neuer Schlag gegen die Bemühungen Verbraucher zu schütze. Die Untersuchung von „Digital Citizens“ ergab, dass Apps, die auf Streaming-Geräte heruntergeladen wurden, die Benutzer einem viel höheren Risiko eines Malwarebefalls im Heimnetzwerk aussetzen.

Die Akteure stehlen alle Daten aus den Geräten im Heimnetzwerk. Einschließlich die der Dienste wie Netflix- und Amazon-Konten.

Die Malware sucht nach dem Weg zu jedem angeschlossenen Gerät und gefährdet so ein ganzes Heimnetzwerk. Die Erweiterung der Infektionsvektoren (die Wege vom Computer eines Angreifers zu verbundenen Geräten im Netzwerk eines Benutzers - wie z.B. ein Kindertablet, ein neuerer Kühlschrank oder ein Computer) erhöht die Wahrscheinlichkeit eines Datendiebstahls.

Die durch Dark Wolfe identifizierte Malware stammt von Apps, die entweder bereits bei der Entwicklung infiziert, über Updates infiziert , oder über den Stream infiziert wurden. Sobald sie im Netzwerk ist, fügt Malware alle lokal gespeicherten Medien hinzu, die sie im Netzwerk der miteinander verbundenen Geräte eines Benutzers findet und macht sie zu einem Teil seines Medienkatalogs, einschließlich der Filme, Bilder und Anwendungen des Benutzers. Selbst wenn das illegale Gerät später aus dem Heimsystem entfernt wird, bleibt Malware, die bereits benachbarte Systeme infiziert hat, im Netzwerk des Benutzers.

Die Ermittler haben zwei Möglichkeiten identifiziert, wie Kriminelle die gestohlenen Daten monetarisieren um die eigenen Taschen füllen. Der erste ist der Verkauf der Anmelde-informationen eines legitimen Benutzers. Gefälschte Netflix-Anwendungen, wie "FreeNetflix", erleichtern den illegalen Zugriff auf ein legitimes Abonnement und ermöglichen es einer Person, die nach nicht lizenzierten Inhalten sucht, auf das Raubkopien-Abonnement eines legitimen Benutzers zuzugreifen. Die Betreiber von FreeNetflix bieten den Service für eine einmalige Zahlung von 10 US-Dollar an. Inklusive aller Updates. Rotierende Log in-Informationen helfen Betreibern von „FreeNetflix“mehrere mögliche Probleme zu vermeiden, einschließlich der möglichen Über-belegung des Abonnements eines einzelnen legitimen Benutzers durch mehrere illegale Benutzer auf einmal. Dadurch wird vermieden, dass der Dienst legitimer Benutzer wiederholt unterbrochen wird, wodurch erzwun-gene Ausfälle, Passwortänderungen und Kontosperren reduziert werden.

Gefälschte Netflix-Anwendungen ergän-zen auch die legitimen Netflix-Streams und bieten zusätzliche Inhalte, die nicht in der eigenen Anwendung von Netflix zu finden sind, einschließlich raub-kopierter Streams von Sportereignis-sen, Musik, Spielen und sogar einigen selbst erstellten Inhalten, was sie sehr begehrenswert macht.

Andere Forscher haben herausgefun-den, dass Addons von Drittanbietern für Kodi verwendet wurden, um Linux- und Windows-Krypto-Währungs-Mining-Malware zu verteilen. "*Die Malware hat eine mehrstufige Architektur und setzt Maßnahmen ein, um sicher-zustellen, dass ihre endgültige Nutzlast - der Kryptominer - nicht leicht auf das bösartige Addon zurückzuführen ist*", berichtete das Sicherheitsunternehmen

ESET in einem Bericht vom September 2018.

Während die Quellen der Malware veraltet waren, oder keine Malware mehr verbreiteten, warnte ESET davor, dass "unwissentliche Opfer", die die Kryptominer-Malware heimlich auf ihren Geräten installiert hatten, wahrscheinlich immer noch betroffen sind.

Piraterie-Mediaplayer oder Set-Top-Boxen sind besonders anfällig für Malware, da typische Sicherheits-vorkehrungen selten installiert oder einfach deaktiviert werden, um Pirate-rie-Streaming-Anwendungen zu er-möglichen. Die Geräte verfügen über deutlich mehr "Angriffsvektoren" als andere angeschlossene Geräte, wie z.B. Smart TVs oder Kühlschränke, was das Risiko erhöht, dass Hacker auf Benutzernamen oder Passwörter für alles zugreifen können, womit das Gerät verbunden ist, wie z.B. Netflix-Konten, Amazon-Konten oder alles andere, was dem System hinzugefügt wurde.

So funktioniert es typischerweise

In dem Moment, in dem ein Benutzer einen „voll geladenen“ Mediaplayer einschaltet und eine illegale App - wie Mobdro, FreeNetflix, Exodus oder Krypton - verwendet, befindet sich die Anwendung nun hinter der Firewall im vertrauenswürdigen Netzwerk und umgeht die Netzwerksicherheit effektiv.

Nach dem Start wird die App sofort und automatisch aktualisiert. Diese Updates sind erzwungen - der Benutzer hat keine Möglichkeit die Änderungen zu blockieren. Alles scheint wie geplant zu funktionieren, aber der Bedrohungsakteur bekommt auch das, was er will - den Zugriff auf das Gerät und die potenziellen Geräte und Netz-werke darüber hinaus. Während der Benutzer denkt alles sei sicher, wird das Gerät des Benutzers tatsächlich mit gefährlichen Waffen ausgestattet. Cybersicherheitspraktiker bezeichnen dies als "erweiterte Funktionalität".

Zum Beispiel, kurz nachdem ein Dark Wolfe-Forscher Mobdro herunter-geladen hatte, leitete er den Wi-Fi-Netzwerknamen und das Passwort des Forschers an einen Server weiter, der in Indonesien zu sein schien. Forscher weisen darauf hin, dass das Endziel trüb ist, weil die Bedrohungsakteure ein virtuelles privates Netzwerk nutzen, das ihren tatsächlichen Standort ver-schleiert. Sobald die App gestartet wurde, berichtete der Forscher, dass

die App ein Update erzwungen hat. Dann begann Mobdro, den Zugang zu Medieninhalten und anderen legitimen Apps im Netzwerk des Forschers zu suchen.

Ein Befund von Dark Wolfe ist besonders beunruhigend Nach dem ersten Update akzeptierte das Gerät Befehle von einem Hacker. Diese Befehle können von der App selbst oder von den Filmstreams kommen. Mit jeder Auswahl von Inhalten öffnet der Benutzer die Tür zu einem neuen Befehlssatz und bösartigen Nutzlasten von einem Hacker zu einem verwendeten Gerät. Dies kann alles umfassen, von Befehlen zum Ausführen eines Updates, um mehr Malware herunterzuladen, an einem DDoS-Angriff teilzunehmen oder auf dem Gerät gespeicherte Elemente - wie Bilder, Filme, Dokumente - oder ähnliche Inhalte, die auf Geräten verfügbar sind, die mit einem Netzwerk verbunden sind.

Mit diesen Tools hat der Hacker nicht nur vollen Zugriff auf die ungesicherten Daten, sondern kann sich buchstäblich so in das Gerät eines Benutzers einloggen, als ob er oder sie davorsitzen würde. Der Hacker kann von diesem Gerät aus im Internet navigieren und sich als Benutzer ausgeben.

Nach der Installation sucht die App nach Updates. Dann agiert die Malware aus den Apps. Forscher beobachteten, dass die App, die die WLAN Daten des Benutzers an einen externen Server in Indonesien schickte, dann anfing, das Netzwerk zu untersuchen um mit allen File-Sharing-Diensten im Local Area Network zu kommunizieren.
Es wurde auch "port knocked", - ein Prozess zur Suche nach anderer aktiver Malware - entdeckt.

Die App nahm auch die Streamdaten auf. Streams können Befehle enthalten, die es Hackern ermöglichen, die Anwendung aus der Ferne zu steuern. Wenn die App auf einem Jailbreak-Gerät läuft, könnte die App heimlich Audio und Video von einem Smart TV beziehen. Die Befehle könnten der App auch sagen, dass sie von einer anderen Quelle aktualisieren soll, wodurch mehr Malware-Funktionalität zur Verfügung steht. Dies ist eine einfache Möglichkeit für Hacker, in Netzwerke einzudringen und die Sicherheit zu umgehen.

Die Forscher von „Digital Citizens“ beobachteten Fälle, in denen nicht lizenzierte Filme und Fernsehsendungen als Köder benutzt wurden, wodurch die Benutzer dazu gebracht wurden, Anwendungen herunterzuladen, die ihre Geräte infizieren.

Die Forschung ergab, dass der Inhalt nicht nur ein Köder ist, sondern auch zur Steuerung und Manipulation von Geräten verwendet wird, die mit dem Netzwerk eines Benutzers verbunden sind.

Auf der Suche nach einem Piraten-Drehbuch

Was die Forscher entdeckten, spiegelt einen gemeinsamen Modus Operandi wider, der von Hackern verwendet wird. In früheren Berichten über adsupported Piraten-Websites berichteten DCA und das Cybersicherheitsforschungsunternehmen RiskIQ über Partnerschaften, bei denen Piratenbetreiber mit Bedrohungsakteuren über den Preis von Malware-Installationen im Dark Web verhandeln.

Was Hacker im Dark Web diskutieren, ist oft ein Frühindikator für die Bedrohungen, denen Verbraucher in Zukunft ausgesetzt sein werden. Um zu verstehen, was als nächstes kommen könnte, stöberten Analysten des Cybersicherheitsunternehmens GroupSense im Dark Web herum, um zu begreifen, welche Bedrohungen in Zukunft anstehen.

Ein Teil der Diskussion im Dark Web konzentrierte sich auf die Nutzung der Malware zur Nutzung der Rechenleistung des Geräts (z.B. zum Angriff auf andere Computer) oder auf den Zugriff auf Informationen, die auf dem Gerät selbst gespeichert sein können (einschließlich Fotos, Passwörter und Kreditkarten). Die Ermittler entdeckten, dass Bedrohungsakteure eine Möglichkeit sehen, Piraterie Anwendungen zu modifizieren, um die Benutzernamen und Passwörter offenzulegen, die Benutzer für den Zugriff auf ihre Geräte und den Inhalt auf diesen Geräten gewählt haben.

Dies ist beunruhigend, da viele Internetnutzer auf einen einzigen Benutzernamen und ein einziges Passwort für mehrere Geräte, Plattformen und Websites angewiesen sind. Angenommen, "sallyjennings" verwendet das gleiche "ilovedogs123!" Passwort für ihr Pirateriegerät sowie für ihren Computer und ihr Heim-Wi-Fi-Netzwerk.

Im Dark Web fand GroupSense konkrete Beispiele für potenzielle Hacker, die nach Malware-Tools für Kodi suchen.
Diese Exploits beinhalteten:

- Ein Exploit-Tool namens "17.0 Local File Inclusion", das es Hackern ermöglicht, auf die Inhalte eines Benutzers über eine Kodi-Box zuzugreifen, die auch persönliche Fotos

und Videos sowie andere Mediendateien enthalten kann.

- Ein Exploit-Tool namens "Kodi 15 Arbitrary File Access", das es Hackern ermöglicht, eine Sicherheitsschwachstelle auszunutzen, um auf sensible Informationen auf dem Gerät eines Benutzers zuzugreifen.
- Ein Distributed Denial of Service (DDoS)-Virus namens "Kodi Web Server 16.1", der es einem Hacker ermöglicht, einen Angriff auf Kodi-Boxen über das Netzwerk und die Bandbreite eines Benutzers durchzuführen.

Bei der Untersuchung der Risiken der mit diesen Geräten verbundenen Malware fand GroupSense die folgenden Bedrohungen für Verbraucher im Zusammenhang mit Bedrohungsakteuren, die auf Piraterieanwendungen abzielen:

- Angriffe, die es einem Hacker ermöglichen, den Datenverkehr abzufangen und zu überwachen. Als "Man-in-the-Middle-Angriff" bezeichnet, glaubt ein Benutzer, dass er sich beispielsweise mit einem legitimen Dienst verbindet, um per Kreditkarte zu bezahlen, aber tatsächlich beobachtet ein Hacker die Verbindung. Auf diese Weise können Passwörter, Kreditkarten und andere Informationen gestohlen werden.
- Kodi Addons setzen Benutzern auch Malware aus, die Bedrohungsakteuren Zugriff auf alle Arten von Inhalten gibt, entweder auf Kodi oder über Kodi. Da Kodi von vielen Verbrauchern als "Medienorganizer" verwendet wird, können sie oft über ihre Kodipowered-Geräte auf persönliche Bilder und Videos zugreifen. Und da diese Geräte immer ausgereifter sind, werden sie wahrscheinlich als Portal für den Zugriff auf andere persönliche Inhalte genutzt.

Die in den Rogue-Apps entdeckte Malware suchte die Erlaubnis, Zugang zu anderen Android-Apps zu gewähren, die der Forscher - der Reverse Engineering für Android-Apps erstellt und unterrichtet - noch nie zuvor gesehen hatte. Die Forscher fanden auch Rogue-Apps, die von Videos stammen, die entweder von Torrents oder von Websites außerhalb der Vereinigten Staaten heruntergeladen wurden und die hochinvasive Malware lieferten, die "Port Knocked" und nach anderer Malware suchten.

Das heißt, sie suchten nach anderen Filmquellen und Dateien im Netzwerk der Forscher und "sprachen" mit den Fernsehern im Netzwerk.

Fazit

Das Ecosystem der Streaming-Piraterie basiert auf Geld verdienen durch Diebstahl. Der Benutzer wird nicht über die Risiken informiert. Benutzer dieser Software werden dazu verleitet, etwas auszuprobieren, von dem sie denken, dass es kostenlos oder billig ist, das aber mit extrem hohen Kosten verbunden ist: Malware die auf Datenklau aus ist.

Darüber hinaus sind die zahlreichen Online-Chats darüber, wie man Kodi-Addons infiziert, und die Diskussionen über Geschäftsmodelle wie man profitiert, rote Flaggen, die signalisieren, dass das Problem wächst.
Auch in Deutschland!

Mediaplayer an sich sind eine feine Sache. Auch wenn es noch so reizvoll ist, der Benutzer sollte sich hüten Apps wie MOBDRO oder FreeNetflix herunterzuladen. Allein schon der Download öffnet den Hackern ein paar Türen. Mehr Türen öffnen sich ihnen, wenn die Apps aktiviert werden.

Und wenn Sie Glück haben wurde Ihre Kreditkarte noch nicht leergefegt, doch Sie bekommen dann die Mail unten:

Betreff: Das ist meine letzte Warnung!
Datum: Mon, 14 Jan 2019 10:55:55 +0000
Von: Anonymer Hacker - Sigrid <sigrid_236@tt.anonymer-hackers.cf>
Antwort an:sigrid_236@tt.anonymer-hackers.cf
An:

LETZTE WARNUNG
Weil Sie mich nicht pünktlich bezahlt haben, müssen Sie jetzt doppelt so viel bezahlen!
Ich gebe Ihnen die letzten 72 Stunden, um die Zahlung zu tätigen, bevor ich ein Video mit Ihrer Masturbation an alle Ihre Freunde schicke.

Das letzte Mal, als Sie eine p0rnografische Website mit Teenagern besucht haben, haben Sie Software heruntergeladen und installiert, die ich entwickelt habe.

Mein Programm hat Ihre Kamera eingeschaltet und den Prozess Ihrer Masturbation aufgezeichnet. Meine Software hat auch alle Ihre E-Mail-Kontaktlisten und eine Liste Ihrer Freunde auf Facebook heruntergeladen.
Ich habe sowohl die lt8b63om.mp4 mit Ihrer Masturbation als auch eine Datei mit all Ihren Kontakten auf meiner Festplatte.
Sie sind sehr pervers!

Wenn Sie wollen, dass ich beide Dateien lösche und das Geheimnis behalte, müssen Sie mir Bitcoin-Zahlungen schicken. Ich gebe Ihnen 72 Stunden Zeit.
Wenn Sie nicht wissen, wie man Bitcoins sendet, besuchen Sie Google.

Senden Sie sofort 2000 EUR an diese Bitcoin-Adresse:
3FtLgWSLg4Jp4bpL5ahiUSBGYjeKE888bB

1 BTC = 3040 EUR, also genau 0.667839 BTC an die obige Adresse senden.

Versuchen Sie nicht, mich zu betrügen! Sobald Sie diese E-Mail öffnen, werde ich wissen, dass Sie sie geöffnet haben.

Diese Bitcoin-Adresse ist nur mit Ihnen verknüpft, also werde ich wissen, ob Sie den richtigen Betrag geschickt haben.
Wenn Sie die Zahlung nicht abschicken, schicke ich Ihr Masturbationsvideo an
alle Ihre Freunde aus Ihrer Kontaktliste, die ich gehackt habe.

Hier sind noch einmal die Zahlungsdaten:

Senden Sie 0.667839 BTC an diese Bitcoin-Adresse:

3FtLgWSLg4Jp4bpL5ahiUSBGYjeKE888bB

Sie können die Polizei besuchen, aber niemand wird Ihnen helfen.
Ich lebe nicht in Ihrem Land. Ich habe diese Nachricht in Ihre Sprache übersetzt, damit Sie sie verstehen können.

Betrügen Sie mich nicht! Vergessen Sie nicht die Scham und wenn Sie diese Botschaft ignorieren, wird Ihr Leben ruiniert.

Ich warte auf Ihre Bitcoin-Zahlung.

Sigrid
Anonymer Hacker

(*1) Über die Digital Citizens Alliance

Die Digital Citizens Alliance ist eine gemeinnützige Organisation, die eine verbraucherorientierte Koalition ist, die sich darauf konzentriert, die Öffentlichkeit und die politischen Entscheidungsträger über die Gefahren aufzuklären, denen die Verbraucher im Internet ausgesetzt sind. Digital Citizens möchte einen Dialog über die Bedeutung führen, die das Internet für die Interessengruppen - Einzelpersonen, Behörden und Industrie - hat, um das Internet sicherer zu machen.

(*2)Über Dark Wolfe Consulting

Dark Wolfe Consulting ist ein Cybersicherheitsunternehmen, das spezialisierte und kommerzialisierte Netzwerksicherheitsbewertungen, Schwachstellenbewertungen, Netzwerkdurchdringungstests, Anwendungsbewertungen und Anwendungsdurchdringungstests anbietet

TBS

TBS-TECHNOLOGY.DE

Entdecken Sie unsere Produktvielfalt!

Multituner

DVB-S2/-S/-S2X/-T/-T2/-C/-C2

Die TBS-5520SE Single-Tuner USB-Box

DVB-S2X

Professionelle TV-Karten

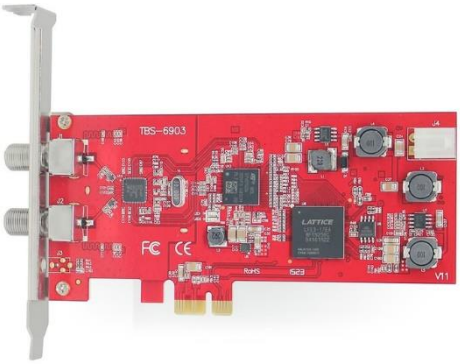
Die TBS-6909-X Octa-Tuner TV-Karte

Tuner für Eumetcast

TV-Tuner und -Boxen für die Verwendung von Eumetcast

Die TBS-5927 Single-Tuner Profi USB-Box

oder die TBS-6903 Doppel-Tuner Profi TV-Karte



Sonderangebote und weitere Produkte finden Sie unter: www.tbs-technology.de

TBS GmbH · Finkenstraße 73 · 67661 Kaiserslautern · Tel: 06301 615910

Mail: info@tbs-technology.de

AIRSPY

Kurzvorstellung

Die Airspy-Hardware

Der Airspy R2 ist eines der bekanntesten SDRs auf dem Markt. Es bietet durchgehenden Empfang von 24 bis 1800 MHz und eignet sich damit für den Empfang und die Analyse von einer Vielzahl von Signalen im VHF und UHF Bereich.

Um die gesamte Kurzwelle (plus Mittel- und Langwelle) empfangen zu können, wird ein optionaler HF-Converter Spyverter angeboten, der genau auf den Airspy abgestimmt ist.

Für Anwendungen, bei denen der verfügbare Platz sehr begrenzt ist, bietet Airspy mit dem Airspy-Mini ein SDR im üblichen USB-Stick Format an. Die Leistungsdaten sind ähnlich dem des großen R2, allerdings entfallen aus Platzgründen einige Komponenten.

Airspy + SDR# = ideale Kombination

Die echte Leistungsfähigkeit eines SDRs ergibt sich - wenig überraschend :) - aus der Software. Der Hersteller des Airspy ist die gleiche Firma, die auch das weit verbreitete SDR# (SDR sharp) Programm anbietet. Durch diese Kombination von Hard- und Software ergeben sich Möglichkeiten und Leistungsdaten, die andere Hersteller so nur schwer bieten können.

Die SDR# Software ist nicht ohne Grund zu einem der beliebtesten Programme bei den SDRs geworden. Leicht zu bedienen und hervorragend in der Übersichtlichkeit bietet SDR# eine Vielzahl an Funktionen. Die Plugin-Architektur erlaubt anderen Autoren zusätzliche Funktionen einzubauen, der Anwender kann sich das Programm nach seinen Bedürfnissen zusammenstellen. Durch die gemeinsame Entwicklung von Hard- und Software ist immer ein problemloses Zusammenspiel zwischen Airspy und SDR# gewährleistet.

Airspy R2 Beschreibung

Der Airspy R2 Receiver verwendet den weit verbreiteten Tuner-Chip R820T2 von Rafael Electronics. In Kombination mit einem leistungsfähigen 32-Bit Cortex ARM Prozessor und einem schnellen 12-Bit AD-Wandler kann der Airspy aus diesem Tuner weitaus mehr 'rausholen' als die üblichen DVB-T Sticks mit RTL Chipsatz. So kann der Prozessor beispielsweise eine größere Datenmenge verarbeiten, das steigert die maximal darstellbare Spektrumsbreite auf ca. 10 MHz (9 MHz aliasfrei).

Der Cortex-Chip ist ebenfalls für den Betrieb des USB-Interfaces verantwortlich. Hier wird eine USB 2.0 Schnittstelle auf dem Computer vorausgesetzt.

Der SDR besitzt einen speziellen Taktgenerator mit einem sehr geringen Phasenrauschen und mit einer Genauigkeit von ±0.5 ppm.
Das geringe Phasenrauschen verbessert den Dynamikumfang und ist wichtig für die Empfindlichkeit des Empfängers.

Besonders interessant für bestimmte Anwendungen ist die Möglichkeit beim Airspy-R2 einen externen Takt einzuspeisen. So kann man ein Rubidium- oder ein GPS-Frequenznormal verwenden, um genaueste Messungen zu machen, oder mehrere Empfänger miteinander zu korrelieren. Verschiedene GPIO Ports können angesteuert werden, um zum Beispiel externe Geräte zu steuern.

Auf der Antennenseite kann eine Versorgungsspannung (4.5V, max. 50mA) optional zugeschaltet werden um einen externen Converter oder Vorverstärker nahe der Antenne zu versorgen.

Ein weiteres wichtiges Merkmal ist die offene Dokumentation der Software-Schnittstellen (API). Auch wenn man selbst kein Programmierer ist, so profitiert doch jeder Anwender davon. Denn nur durch eine offene Architektur ist gewährleistet, dass andere Programm-Autoren in der Lage sind, eigene Software zu schreiben oder anzupassen. Ein Beispiel dafür sind die ExtIO DLLs oder Treiber für andere Betriebssysteme. Auch die Firmware des verwendeten ARM Prozessors liegt im Quelltext vor und ermöglicht so eigene Anpassungen.

SDR# (SDR Sharp) Software

Die SDR# Software kommt aus dem gleichen Haus wie der Airspy-Empfänger. Durch die gemeinsame Entwicklung ist ein perfektes Zusammenspiel der beiden Komponenten gewährleistet.

Nicht umsonst hat sich SDR# zu einem der beliebtesten Programme für verschiedene SDRs entwickelt.

Das Programm ist einfach zu bedienen, bietet aber durch seine Plugin-Architektur eine hervorragende Erweiterbarkeit. So stehen neben den Grundfunktionen des Programmes selbst Erweiterungen für das Speicher-management, für den Scannerbetrieb oder verschiedene Decoder zur Verfügung.

Natürlich kann man auch externe Decoder mit SDR# betreiben.
SDR# ist kostenlos und kann frei von der Webseite des Herstellers des Airspy geladen werden. Dort findet man auch Links zum Support, z.B. den #airspy Kanal im IRC.

http://airspy.com/download/

Bezugsquelle

WiMo Antennen und Elektronik GmbH

Am Gäxwald 14

76863 Herxheim

Telefon: +49 (0)7276 9668–0

Telefax: +49 (0)7276 9668–11

E-Mail: info@wimo.com

Internet: www.wimo.com

GEWINNSPIEL

Gewinnspiel für alle Abonnenten

Überraschungspaket von VU+ !

Zur Teilnahme beantworten Sie die folgende Frage richtig:

Der VU+ Ultimo 4K kommt mit einem DVB-S2 FBC Twin Tuner. Wie viele Programme kann man damit gleichzeitig aufnehmen, ansehen oder streamen?

Suchen Sie die Antwort auf www.hm-sat-shop.de

Schicken Sie uns Ihre Lösung bitte an ***gs@tectime.tv*** **bis zum 31. August 2019**.

Der Rechtsweg ist ausgeschlossen. Der Veranstalter weist darauf hin, dass sämtliche personenbezogenen Daten des Teilnehmers ohne Einverständnis weder an Dritte weitergegeben noch diesen zur Nutzung überlassen werden.

Verbreitung und Abonnements

Direkt

www.tectime.tv
magazin@tectime.tv

United Kiosk

https://www.united-kiosk.de/zeitschriften/audio-film-foto/tectime-magazin-epaper/ebinr_2117112/

www.tectime.tv

magazin@tectime.tv