TecTime Magazin

Ausgabe 14

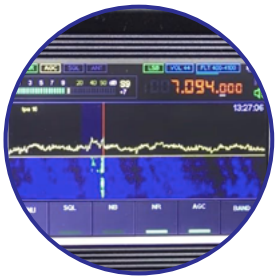
GEWINNSPIEL: VU+ und nixplay

TEST
Gigablue
UHD Trio 4K

TEST
NVIDIA
Shield TV

INTERNET
6 Tipps für die
IT-Sicherheit

US-Luftwaffe erlaubt Hackern einen umlaufenden Satelliten zu entführen



SDR
Malachit-DSP

Raspberry Pi SERIE
Vier aktuelle
Raspberry-Pi-
Alternativen

NOSTALGIE
Vor 21 Jahren

INHALT

EDITORIAL

Christian Mass

Chefredakteur

Liebe Leser,

erste einmal ein wenig Geschichte. In meinen Haushalt zog das Satelliten TV im Jahre 1984 ein. Die erste Anlage bestand aus einem DX-Receiver aus Japan, einer 1, 5 Meter Offset-Antenne desselben Herstellers und einen DX-LNB (damals für 1.600, - DM zu haben). Es gab nur eine Polarisation. Entweder vertikal oder horizontal. Je nachdem wie man den LNB drehte. Zu empfangen waren einige Programme auf 66 Grad und 63 Grad Ost, den sowjetischen Staatssender auf 14 Grad West und weitere Sender über ECS (dem Vorläufer des HOTBIRD) auf 13 Grad Ost. Wir waren damals eine kleine Gruppe von ungefähr 12 Leuten in Europa, die sich gegenseitig Infos über neu entdeckte Sender per Fax zusandten. Dann 1987 kann Peter Lepper mit seiner bis dahin unbekannten Firma TechniSat ins Spiel. Stolz präsentierte er auf einer Hausmesse die ersten „eigenen" Produkte. Bei näheren hinabsehen erschienen sie uns gar nicht so „eigen", denn der Receiver war in Wirklichkeit ein Drake aus den USA, die beiden LNB´s (vertikal und horizontal) kamen vom Hersteller NEC und die Antenne wurde durch SONIM entwickelt und produziert. Unsere zynischen Kommentare dazu vernahm Peter Lepper nicht gerade mit Freude. Verziehen hat er mir das wohl nie. Nichtsdestotrotz sollte Peter Lepper und seine TechniSat den deutschen Markt gründlich umkrempeln und das Satellitenfernsehen hoffähig machen. Mit dem am 11. Dezember 1988 gestarteten Astra 1A-Satelliten begann der Boom. Und der zog sich mit Höhen und Tiefen bis in das Jahr 2018 hin. Die Streamingdienste (hier vor allen Dingen Netflix und Amazon Prime) veränderten und verändern immer noch das Sehverhalten. Vor allem in den Ballungsgebieten mit ausreichend schnellem Internet. In der Fläche mit Internetanbindungen, die eher an die dritte Welt erinnern, bei älteren Menschen und bei Linux-Enthusiasten hat das Satelliten-TV jedoch noch immer einen hohen Stellenwert. Dieses Medium zeichnet sich nach wie vor als qualitativ führend aus. Die sehr gute Bildqualität und keine laufenden Kosten lassen da das Kabel alt aussehen. Hinzu kommt ein breites Informations-Angebot, dass die Streamingdienste noch nicht liefern. Was fehlt, sind Innovationen seitens der Hersteller von Set Top Boxen. Dass Qualität und Innovationen belohnt werden, zeigen die Produkte von VU+ und Gigablue, die trotz der allgemeinen Umsatzrückgänge ihren Marktanteil halten können.

Herzlichst,

Euer Dr.Dish

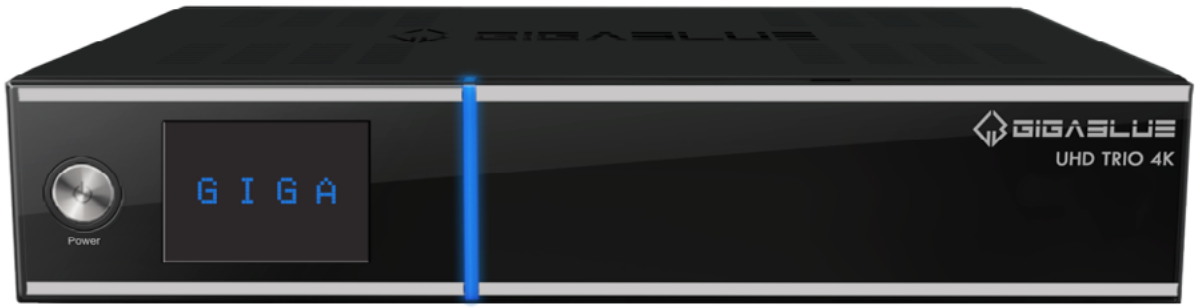
Impressum

Herausgeber, Chefredakteur und verantwortlich für den Inhalt

Christian Mass | mass@tectime.tv | Rosenheimer Landstrasse 69B, 85521 Ottobrunn

Gigablue UHD Trio 4K

Im Test



Mit dem GigaBlue UHD Trio 4K bietet die bekannte Receiver-Schmiede eine preisgünstige UHD Combo-Set Top Box mit einem Linux-Betriebssystem auf Enigma2-Basis an. Für wenig Geld kann der Nutzer die Vorteile von Enigma 2 nutzen. Plugins erweitern die – fast schon endlosen – Funktionen dieser Set Top Box und da der Gigablue UHD Trio 4K über Multiboot verfügt, akzeptiert er weitere Images.

Warum jedoch sollte man sich einen Kombi-Receiver mit Tunern für DVB-SX2, DVB-S und DVB T2 kaufen? Nun, denken wir an den Winter. Der Spiegel draußen ist eingeschneit und nichts geht mehr. Oder das das Sat-Signal fällt bei extremen Wetterlagen (und die kommen immer öfter) aus. Mit einem Kombi-Receiver wird einfach auf eine alternative Empfangsart geschaltet und schon geht es weiter. Oder es wird geplant in Zukunft von DVB T2 oder C auf Satellit umzusteigen, dann spart man sich den Neukauf eines Sat-Receivers.

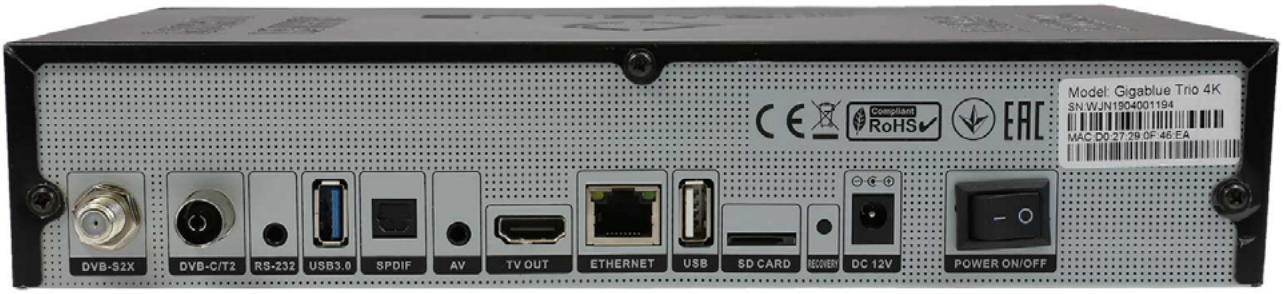
Nach diesem kurzen Überblick sehen wir uns diesen Gigablue UHD Trio 4K etwas genauer an. Mit den Ausmaßen von 280 mm x 175mm x 55 mm kann man den Gigablue getrost als kompakt bezeichnen. In der transportsicheren Verpackung finden wir den UHD Trio 4K , die Fernbedienung, Batterien, ein HDMI-Kabel und das Benutzerhandbuch.

Die Fernbedienung macht Dank der gebürsteten Oberflache einen wertigen Eindruck. Sie ist für drei weitere Geräte programmierbar und sorgt somit für Ordnung auf dem Couchtisch. Die Tasten sind gut ablesbar und haben einen angenehmen Druckpunkt.

Die Vorderfront des Gigablue UHD Trio 4K wird auf der linken Seite von der Standby-Taste, einem gut ablesbaren LC-Display, dass im Standby-Modus die Zeit anzeigt und im Betrieb die Programmnummer und einer senkrechten LED-Leiste beherrscht. Die Helligkeit des Displays lässt sich über das Menü einstellen.

Unter einer Klappe verstecken sich die Tasten für die Bedienung direkt am Gerät. Hier finden wir auch einen USB 2.0 Port und einen Conax-Kartenleser. Eine CI-Schnittstelle gibt es nicht.

Auf der Rückseite befinden sich die Antenneneingänge für DVB S2X und DVB-C/T2. Zwei weitere USB-Ports (2.0



und 3.0) erleichtern die Einbindung externer Geräte wie z.B. eine Festplatte. Die Internetanbindung erfolgt über die LAN-Schnittstelle, oder aber über einen optionalen WIFI Dual Band Stick (1200

Mbps) von Gigablue. Der Flachbildschirm findet seine Einbindung an dem HDMI-Port und das digitale Audiosignal kann vom optischen S/PDIF-Ausgang abgegriffen werden. Wer´s analog mag, dem stehen Audio und Video an einer Klinkenbuchse zur Verfügung. Abgerundet wird die ganze Sache durch einen SD-Kartenleser. Natürlich gibt es einen Netzschalter.

Die Technik

Der GigaBlue UHD Trio 4K ist mit einem 15.000 DMIPS starken 1.600 MHz ARM Cortex A53 Quadcore 64 Bit Prozessor ausgestattet und verfügt über einen ein Gigabyte DDR-4 RAM Arbeitsspeicher, sowie acht Gigabyte MMC Flash-Speicher. Über den SD-Kartenleser lässt sich der Flash-Speicher des Receivers erweitern. Eine darin steckende Micro-SD-Karte kann stattdessen aber auch als Speicher für Aufnahmen genutzt werden. Der Gigablue UHD Trio 4K kann Bilddateien der Formate JPEG, BMP, GIF und PNG, Audiodateien der Formate MP3, FLAC, M4A und WAV sowie Videodateien der Containerformate AVI, M4V, MKV, MOV, MP4, MPEG, TS, VOB und WMV wiedergeben.

Die Tuner sind fest verbaut und können nicht gewechselt werden. Bei DVB-C und T2 handelt es sich um einen Kombi-Tuner. Der DVB-S2X Tuner bietet eine Multistream-Unterstützung. Das heißt, er kann Programmpakete verarbeiten, die nicht unbedingt für den Endkunden gedacht sind. So z.B. Zuspielungen für DVB-T Sendestationen. Der Gigablue UHD Trio 4K ist Multiboot-fähig. Es können neben dem vom Hersteller aufgespieltem Enigma2-Image weitere installiert werden. Die Wahl des

gewünschten Images erfolgt beim Boot-Vorgang.

In der Praxis

Angst vor Linux, da zu kompliziert? Diese Angst ist beim UHD Trio 4K unbegründet, denn ein Installations-Wizzard führt auch den Laien unkompliziert durch die ganze Erstinstallation. Unicable und DiSEqC (1.0, 1.1, 1.2) und USALS werden jeder Antennenart gerecht. Der integrierte Satfinder ersetzt ein gutes Antennenmessgerät und erlaubte die präzise Ausrichtung der Antenne.

Um den EPG, Time-Shift oder die Aufnahme auf eine externe Festplatte zu nutzen, bedarf es keiner weiteren Installationen von Plugins. Wer in die spannende Materie tiefer einsteigen will, der findet im Menüpunkt „Erweiterungen“ eine wahre Fundgrube. Unter Picons können durch den Hersteller vorbereitete Picons installiert werden. Unter Settings findet er Nutzer aktuelle Kanallisten. Verschiedene Oberflächen können unter SKINS ausgewählt werden und wichtige System-Plugins sind unter diesem Stichwort zu finden.

Wer lieber über das Handy oder das Tablet seinen UHD Trio 4K kontrollieren möchte, dem steht die Gigablue Player App zur Verfügung. Natürlich kann der Gigablue in ein Netzwerk eingebunden werden. Und wer im ganzen Hause auf allen möglichen Endgeräten Satelliten-Fernsehen empfangen möchte, dem hilft das Gigablue Server Box Plugin auf die Sprünge.

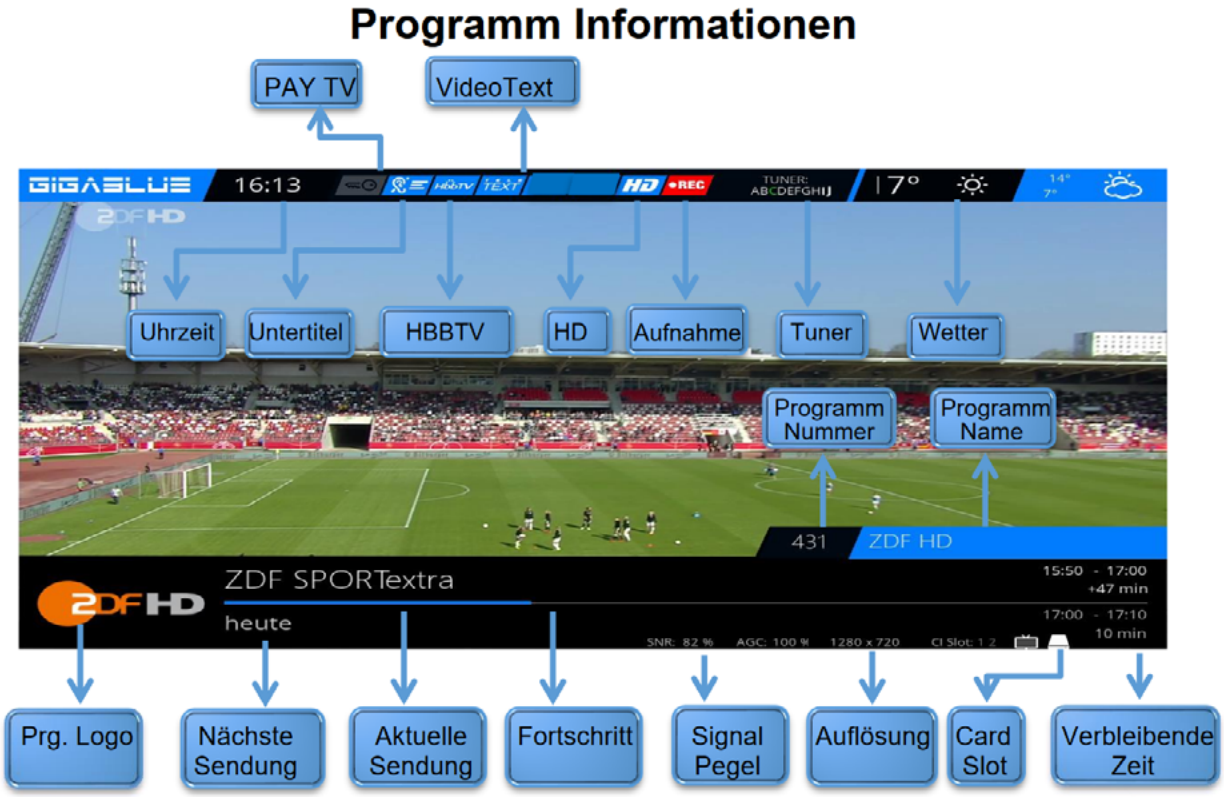
Ein Auszug aus dem sehr gut gemachten Benutzerhandbuch:

„Das GigaBlue Server Box Plugin ist in der Grundsoftware installiert. Wie funktioniert es? Zuerst benötigen Sie ein Heimnetzwerk, indem der GIGABLUE Server und der GigaBlue IP Box Client verbunden sind. Sie müssen miteinander kommunizieren können. Der GIGABLUE Server empfängt die SAT TV, KABEL und terrestrischen TV- und Radio Signale. Die GigaBlue IP Box Clients fordern dann über ein spezielles GIGABLUE IP Kommunikationsprotokoll die SAT, Kabel und terrestrischen Programme vom GIGABLUE Server an. Der GIGABLUE Server konvertiert alle Pro-

gramme in ein IP Signal und stellt diese Signale den GigaBlue IP Box Clients zur Verfügung. Der GIGABLUE Server kann mehrere IP Endgeräte gleichzeitig versorgen. Somit können Sie SAT-Fernsehen auf iPad und Co gleichzeitig schauen. Welche Endgeräte kann ich nutzen? Als Server können Sie nur GigaBlue Geräte nutzen. Bei der Endgerätewahl steht Ihnen eine große Auswahl zur Verfügung. Auf folgenden Geräten können Sie GIGABLUE empfangen: Laptop, PC, Smartphones, Tablets, UPNP/DLNA fähige Mediaplayer, GigaBlue IPTV Set-Top-Boxen oder direkt über den LAN Anschluss an Ihrem Fernseher. Durch die SAT IP Übertragung entstehen keine Bildverluste. Sie können auf den Geräten die volle HD Qualität empfangen. Funktionen wie Videotext, EPG, Audiooptionen und Untertitel stehen zur Verfügung. Auch die Aufnahmefunktion kann genutzt werden. Wie viele Sender kann ich gleichzeitig verteilen? Die Anzahl der gleichzeitig gestreamten Sender hängt von der Qualität des Heimnetzwerkes ab. Bei einem HD Stream werden ca. 20 MBit/s an Daten gesendet. Bei SD sind es ca. 7-10 MBit/s. Wenn Sie eine normale LAN Verkabelung (100 MBit/s) in Ihrem Heimnetzwerk haben, können Sie theoretisch gleichzeitig 20 HD Sender an unterschiedliche Endgeräte schicken. Bei der SD Auflösung wären es 40 Sender. Bei einer 1 GBit/s (1000 MBit/s) LAN Verkabelung erhöht sich der Faktor um bis zu 50“.

Vorteile

1. DVB-S/S2, DVB-C und DVB-T/T2 über IP verteilen und SAT, Kabel und terrestrisches TV auf vielen Endgeräten schauen, die keinen Tuner haben.
2. Sehr gute Bildqualität
3. Der SAT Empfang ist im gesamten Haus möglich
4. Keine zusätzliche Verkabelung ist notwendig
5. Es gibt verschiedene Übertragungswege (LAN, WLAN, PowerLine).



Und das bietet der Gigablue UHD Trio in seiner Grundausstattung:

- 4K/UHD-Auflösung
- Steuerbar über Smartphone und Tablet (via GigaBlue Player-App)
- Aufnahmen via Smartphone, Tablet oder PC von unterwegs programmieren
- Blindscan
- Mit SAT>IP Technologie Satelliten-TV auf mehrere (mobile) Endgeräte übertragen
- Multiroom-fähig
- Multiboot-fähig
- Mit Time Shift Sendungen pausieren oder bis zu 2 Stunden zurückspringen (optional)
- Timer-Funktion
- 14 Tage Elektronischer Programmguide (EPG) mit detaillierter Übersicht
- Firmware Updates über Internet
- Over-The-Air Updates (OTA)
- WLAN-fähig (optional mit GigaBlue WiFi-Stick)

Fazit

Die Verarbeitungsqualität des Gigablue UHD Trio 4K ist sehr gut- Und genauso verhält es sich mit der Ausstattung und Bedienung. Das ausführliche Handbuch ist sowohl für den Laien in der Verständlichkeit als für den Fortgeschrittenen hilfreich. Die Menüführung ist intuitiv. Hervorzuheben ist die wirklich hervorragende Darstellung von UHD-Inhalten. Für 124,99 Euro bekommt der Käufer einen realen Gegenwert.

Anbieter

Impex-Sat GmbH & Co. KG

Beim Gießhaus 7

25348 Glückstadt

Tel.: 04124-937262

Fax: 04124-937266·

info@impex-sat.de·

www.impex-sat.de

GEWINNSPIEL

EXKLUSIV FÜR ALTE UND NEUE ABONNENTEN

1. PREIS: VU+ Ultimo 4K

2. PREIS: nixplay Smart Photo Frame

Um am Gewinnspiel teilzunehmen,
beantworten Sie bitte die folgende Frage richtig:

Wie viele Satelliten sind in der vollautomatischen Satelliten-Antenne Selfsat SNIPE 2 Air SE vorprogrammiert?

Email: mass@tectime.tv

Hier gibt es eine kleine Hilfestellung zur Frage:

https://satco-europe-shop.de/camping/

Der Rechtsweg ist ausgeschlossen.

1

2

TECHNIK

NVIDIA Shield TV

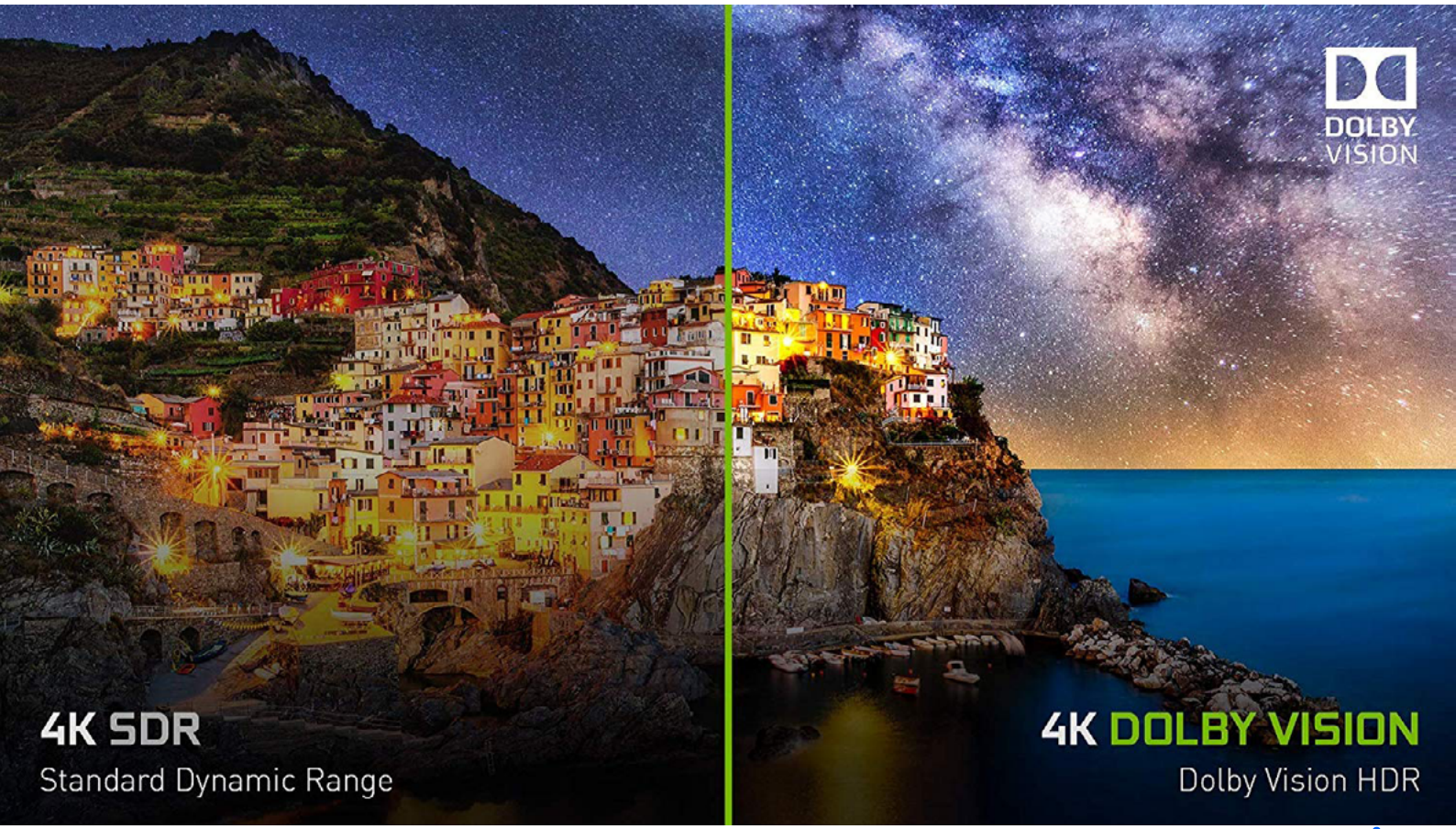
Im Test

Die neuen Nvidia Shield-TV Mediaplayer sind inzwischen beim Fachhandel angekommen.

Zwei Modelle gibt es:
den Nvidia Shield TV Pro für 219,00 Euro, mit einem identischen Design wie das Vorgängermodell, und den brandneuen 159,99 Euro teuren Nvidia Shield TV.

Beide verfügen nun neben HDR10 und Dolby Atmos-Audio auch über Dolby Vision.

Die Fernbedienung wurde komplett neu gestaltet. Das andere neue Feature ist ein KI-gestütztes Upscaling-System, das 1080p-Inhalte detaillierter aussehen lässt und der 4K-Qualität näherkommt.



Nach ein paar Tagen ausführlicher Tests des röhrenförmigen Shield TV entstand der Eindruck, dass dieses Produkt nicht nur die Heimkino-Besitzer anspricht, sondern ein wesentlich breiteres Publikum, das wegen der schieren Leistung des Gerätes und der gut durchdachten Software sich vom Nvidia Shield TV angezogen fühlt.

Sowohl der Shield TV Pro als auch der Shield TV beinhalten den Tegra X1+ Chip von Nvidia, der bis zu 25 Prozent schneller ist, als der Chip des Vorgängers. Der Shield war schon immer stark, wenn es um die Leistung ging und wir glauben nicht, dass man nirgendwo ein schnelleres Android-TV-Erlebnis finden wird. Diese Art von Geschwindigkeit und Fluidität wird nur vom Apple TV 4K übertroffen. Netflix, YouTube, Prime Video und andere Apps öffnen sich fast sofort. Der Google Assistent reagiert schnell und Android TV kann nun in die mit der Google Home App erstellten Routinen integriert werden.

Der Startbildschirm sieht gut aus und ist nicht mit Anzeigen wie bei Roku oder Fire TV bestückt. Uns gefällt, dass man direkt auf dem Startbildschirm durch aktuelle Videos aus dem persönlichen YouTube-Abonnements scrollen kann. Aber nicht viele Apps bieten diese horizontalen Karusselle an. Sprachbefehle über den Google Assistent und Ama

zons Alexa funktionieren zuverlässig. Google verbesserte auch endlich den Play Store auf Android TV für eine einfachere Auffindbarkeit.

Jedes intelligente Gerät verlangt jetzt, dass man einer Reihe von Bedingungen zustimmen muss, bevor man es nutzen kann. Hier eine Liste, die vor der Inbetriebnahme abgearbeitet werden muss:

- Google Nutzungsbedingungen
- Google-Datenschutzbestimmungen
- Google Play Nutzungsbedingungen
- Nvidia Nutzungsbedingungen
- Nvidia Datenschutzerklärung

Die folgenden Vereinbarungen sind freiwillig:

- Standortdaten
- Diagnostik

Endgültige Zählung: fünf verbindliche Vereinbarungen und zwei oder mehr optionale Vereinbarungen.

Das Design des Shield TV ist sicherlich unkonventionell. Man wird dieses Ding nicht mit einem Apple TV oder Roku verwechseln. Und mit über 15,24 Zentimetern Länge ist der Shield TV keineswegs ein Streaming „Stick“. Es ist nicht dazu gedacht am HDMI-Anschluss des Fernsehers zu hängen. Stattdessen glaubt Nvidia, dass die meisten Kunden ihn hinter dem Fernseher verstecken werden.

An beiden Enden des Rohres (anders kann man den Sheiled TV kaum bezeichnen) befinden sich verschiedene Anschlüsse: HDMI, microSD und eine Suchertaste auf der einen Seite und Ethernet und Netzteil auf der anderen

Upscaling **AUS**

Upscaling **AN**

Seite. Der microSD-Steckplatz befindet sich so nah am HDMI-Anschluss, dass der Zugriff mit ziemlicher Sicherheit durch das Gehäuse eines HDMI-Steckers behindert wird, so dass man das Kabel möglicherweise entfernen muss, wenn man eine SD Card mit neuen Filmen oder anderen Inhalten laden möchte. Trotzdem sollte man dem Hersteller danken, dass er hier erweiterbaren Speicherplatz eingebaut hat, da der Shield TV selbst nur 8GB an Bord hat.

Der Shield TV Pro, der über ein traditionelles Set-Top-Box-Design verfügt, bietet den doppelten Speicherplatz (16 GB) und mehr RAM (3 GB statt 2 GB auf dem Shield TV). Diese Zahlen erscheinen uns jedoch immer noch als zu niedrig für ein 219 Euro teures Gerät. Der Pro ist der einzige der beiden, der als Plex Media Server verwendet werden kann, und er hat auch zwei USB 3.0-Ports zum Anschluss externer Laufwerke, Tastaturen/Mäuse oder Samsungs SmartThings Link. Neben dem schnelleren Prozessor und Dolby Vision gibt es wirklich nicht viel Neues, und dem Shield TV Pro fehlt Wi-Fi 6 und HDMI 2.1.

Keine der beiden Versionen wird mehr mit einem Gamecontroller ausgeliefert. Das Shield Gamepad kann weiterhin separat erworben werden und der Shield TV unterstützt auch Sonys DualShock 4 und Microsofts Xbox One Controller. Nvidia's GeForce Now Game Streaming Service ist im Lieferumfang enthalten und ist - vorerst - noch kostenlos während der Beta-Phase. Googles eigener Stadia-Service wird voraussichtlich erst im nächsten Jahr auf Android TV erscheinen.

Die mitgelieferte Fernbedienung wurde erheblich verbessert. Sie verfügt nun über Tasten für Power, Lautstärke und schneller Vor- und Rücklauf. Die Tasten für die Sprachsuche, die Home- und die Retour-Taste sind weiterhin vorhanden und am unteren Rand befindet sich eine spezielle Tastenkombination für Netflix. Netflix ist der einzige Service,

der diese Sonderbehandlung erhält. Auf Anfrage hieß es, die Bevorzugung von Netflix sei der starken Verbreitung dieses Streaming-Anbieters geschuldet.

In der oberen rechten Ecke der Fernbedienung befindet sich eine Schaltfläche, die man anpassen kann, um eine beliebige Anwendung zu öffnen (wir gehen davon aus, dass Plex und Kodi beliebte Optionen sein werden), das Einstellungsmenü zu starten, einen Screenshot zu machen oder eine Vielzahl anderer Möglichkeiten. Die Tasten der Fernbedienung sind hintergrundbeleuchtet und werden aktiviert, wenn eine Bewegung erkannt wird. Sie benötigt zwei AAA-Batterien und verfügt über Bluetooth (zur Kommunikation mit dem Shield) und IR (zur Steuerung des Fernsehers und der Soundbar).

Die Shield Modelle 2019 unterstützen Dolby Vision, HDR10 (nicht HDR10+), Dolby Atmos und Dolby Digital Plus Surround Sound. So findet man viele 4K HDR-Filme und TV-Shows von allen gängigen Verdächtigen. Und die Netflix-App gibt endlich Atmos an den Slield TV aus. Aber es gibt eine Enttäuschung: Der Shield TV wird HDR von YouTube nicht abspielen,

Für alle Inhalte, die nicht in 4K vorliegen, lohnt es sich, die neue KI-gestützte Hochskalierung von Nvidia auszuprobieren. Die Hochskalierung erweckt den Eindruck erwecken, dass man Inhalte in einer höheren Auflösung als das ursprüngliche Quellmaterial ansieht. Alles wirkt klarer und detaillierter. Aber Fernseher und Streaming-Gadgets neigen dazu, einen unterdurchschnittlichen Job daraus zu machen. Nvidia sagt, dass es ein „tief lernendes neuronales Netzwerk“ trainiert hat, um 1080p- und sogar 720p-Videos auf 4K hochzurechnen und es führt dieses neuronale Netzwerk in Echtzeit aus, wenn man Videos auf dem Shield TV und Shield TV Pro abspielt.

Funktioniert das? Ja! Das System von Nvidia macht einen spürbaren Unterschied, und es ist nicht nur eine einfache Überlagerung. Die KI-Hochskalierung funktioniert nicht fbei 60fps-Videos, noch funktioniert

sie bei Spielen. Aber für alles andere kann man die Hochskalierung jederzeit nutzen, um das On-Screen-Bild zu optimieren. Und wir waren sehr beeindruckt.

Der Shield TV 2019 schießt sofort an die Spitze unserer Empfehlungsliste für diejenigen, die ein erstklassiges Streaming-Erlebnis in ihrem Wohnzimmer wünschen. Mit 159,99 Euro nicht gerade ein Schnäppchen, doch dafür bekommt eine durchdachte Software, einen extrem schnellen Mediaplayer und eine tatsächlich funktionierende Hochskalierung.

POSITIV

- Extrem schnell
- Beeindruckendes 4K-Upscaling
- Bessere, ergonomischere Fernbedienung

NEGATIV

- HDR für YouTube ist nicht geeignet.
- Keine signifikanten Hardware-Verbesserungen im Vergleich zum alten Shield TV
- Kein HDR10+, Wi-Fi 6 oder HDMI 2.1

TECHNIK

US-Luftwaffe erlaubt Hackern einen umlaufenden Satelliten zu entführen

Als die Luftwaffe letzten Monat bei der Defcon Hackerkonferenz in Las Vegas auftauchte, kam sie nicht mit leeren Händen. Sie brachte ein F-15-Kampfjet-Datensystem mit. Ein System, das die Hacker gründlich demontiert und dabei schwerwiegende Schwachstellen gefunden haben. Die USAF war mit dem Ergebnis so zufrieden, dass sie sich entschieden hat den Einsatz zu erhöhen. Nächstes Jahr bietet sie den Hackern eines Satelliten an.

Das sah vor einigen Jahren noch ganz anders aus. Als Dr.Dish 1995 die Unsicherheit der US-Kommandosatelliten (damals noch unter dem Namen „Fleetsatcom“) dokumentierte und veröffentlichte, teilte das US- Department of Defence mit, dass man eine neue Generation von Satelliten plane, die dann sicher seien. Und die neue Generation unter dem Namen „UHF-Follow On“ kam und Dr.Dish bewies erneut, dass auch diese hoch sensiblen Satelliten löcherig wie ein Schweizer Käse waren (und es bis heute sind). Die kritische Story kam in den USA gar nicht gut an und bescherte dem Autor zwei Jahre Einreiseverbot in das gelobte Land. Nicht offiziell. Die Warnung erreichte Dr.Dish über einen mit den USA befreundeten Geheimdienst.

Das Versprechen einen Satelliten als Spielball für die Hacker zur Verfügung zu stellen kam von Will Roper, stellvertretender Sekretär der Luftwaffe für Beschaffung, Technologie und Logistik. Hackern den Zugang zu einem aktiven Satelliten im All und den Bodenstationen zu gewähren, scheint ein recht mutiger Schritt zu sein. Jedoch steht dieser Schritt im Einklang mit Ropers Verpflichtung, die Art und Weise, wie seine militärische Dienststelle die neuen Cybersicherheits-Herausforderungen umsetzt.

„Wir müssen unsere Angst überwinden, externe Experten hinzuzuziehen, die uns helfen, sicher zu sein. Wir haben immer noch Cybersicherheitsverfahren aus den 90er Jahren“, sagt Roper. „Wir haben ein sehr geschlossenes Modell. Wir gehen davon aus, dass, wenn wir Dinge hinter verschlossenen Türen bauen und niemand sie sieht oder gar berührt, sie sicher sind. Das mag in einer analogen Welt bis zu einem gewissen Grad zutreffen. Aber in der zunehmend digitalen Welt ist alles Software basiert“. Roper fügt hinzu: „„Was die Hacker tun sollen, ist zu versuchen den Satelliten mit allen Mitteln zu übernehmen“.

Software hat unweigerlich Fehler, die ausgenutzt werden könnten, sei es in einer intelligenten Mikrowelle oder einem komplexen Flugsystem. Roper weiß das aus Erfahrung: Die „Hack the Air Force“ Initiative, die aus einer Partnerschaft zwischen HackerOne und dem Pentagon‘s Defense Digital Service (DDS) entstand, zahlte 130.000 Dollar an Hacker aus, die im vergangenen Dezember insgesamt über 120 Schwachstellen gefunden hatten.

Es war DDS, die die Luftwaffe mit den Organisatoren von Defcon‘s Aviation Village verband, einer Gruppe auf der Hacking-Konferenz, die sich allen militärischen und zivilen Dingen in der Luft und im All widmet. Sieben ausgewählte und sicherheitsüberprüfte Hacker griffen - unter den wachsamen Augen der USAF - eine „Trusted Aircraft Information Download Station“ an, die Daten auf einer F-15 hin und her überträgt. Die Schwachstellen des Systems waren offensichtlich. Die Luftwaffe verfügt natürlich über ein eigenes internes Cyber-

sicherheitsteam, aber deren Ressourcen sind begrenzt. Da braucht es ein wenig Hilfe von außen.

„Sie würden wirklich hohe Sicherheitsvorkehrungen beim Bau der F-15 erwarten und die hat sie auch. Doch viele Komponenten werden von kleineren Firmen entwickelt und gebaut“, sagt Roper „Und Sie können sich vorstellen, dass kleinere Unternehmen ohne die Ressourcen eines Lockheed Martin oder Northrop Grumman oder Boeing sind nicht in der Lage, über Cyber-Resilienz und Sicherheit auf dem Niveau der großen Unternehmen nachzudenken“.

Sobald die Luftwaffe sieht, welche gemeinsamen Sicherheitsfallen die Teile von Drittanbietern plagen, kann sie beginnen, strengere Sicherheitsanforderungen in ihre Verträge aufzunehmen. Das stählt die gesamte Lieferkette - was wiederum die Sicherheit der Flugzeuge aller Beteiligten erhöht.

Es muss jedoch noch mehr getan werden, um die Undurchsichtigkeit der gesamten Luftfahrtindustrie zu beseitigen. Flugzeugteile sind für unabhängige Forscher schwer zu bekommen und die großen Hersteller halten sie gegenüber der unabhängigen Forschung lieber unter Verschluss. „Es ist besonders eklatant in einer Zeit, in der ähnliche Spannungen mit der Automobil- und Medizinprodukt-Branche weitgehend beseitigt sind“, sagt Pete Cooper, Direktor des Aviation Village. „Ich konnte die gleiche Zusammenarbeit im Luftfahrtbereich nicht sehen“, sagt Cooper. „Es gab nicht wirklich viel, was produktive und positive Beziehungen in diesem Bereich ermöglichte.“ Roper hofft, dass die Beteiligung der Luftwaffe helfen kann, diese Brücke zu bauen.

Der Satelliten-Hack

So wird es ablaufen: Die US-Luftwaffe wird einen Aufruf zur Einreichung von Beiträgen veröffentlichen. Wer meint zu wissen, wie man einen Satelliten oder eine Bodenstation hackt, kann mitmachen. Eine ausgewählte Anzahl von Hackern, deren Ergebnisse realisierbar erscheinen, wird eingeladen ihre Ideen während einer „Flat-Sat“-Phase auszuprobieren. Im Wesentlichen ein Testaufbau, der alle möglichen Komponenten umfasst. Das findet sechs Monate vor der Defcon 2010 statt. Die Gewinner aus dieser Gruppe werden dann für den Live-Hacking-Wettbewerb von der Luftwaffe zur Defcon 2020 geflogen. Und dann geht es zur Sache am lebenden Objekt. Schließlich kommt es nicht oft vor, dass man einen Satelliten hacken darf. Und das auch noch ganz legal!

„Wenn Sie in das Nervenzentrum eines Satelliten einsteigen wollen, können Sie es entweder über die Bodenstation bewerkstelligen oder Sie versuchen mit Ihrem eigenen Emitter direkt in den Satelliten zu gelangen. Wir werden die Möglichkeit haben, dass die Teilnehmer beides tun können“, sagt Roper. „Aber was sie tun werden, ist zu versuchen, den Satelliten mit all den Mitteln zu übernehmen, die sie finden.“

Sicherheitsforscher müssen einen Überprüfungsprozess durchlaufen, denn es handelt sich schließlich um militärische Ausrüstung. Aber im Idealfall ist die Gelegenheit den Aufwand wert. Und je früher im Prozess die Sicherheitsgemeinschaft eintritt, desto besser. „Wir wollen uns in das Design hacken, nicht nachdem wir gebaut ha-

ben“, sagt Roper. „Es gibt keinen Grund, es nicht zu tun, Außer der historischen Angst, dass wir Leute außerhalb der Luftwaffe hereinlassen.“

Wenn die Luftwaffe bereit ist, die Leute unter die Haube schauen zu lassen, dann wird es vielleicht auch die zivile Luft- und Raumfahrtindustrie tun. „Was wir erreichen wollen, ist der Industrie zu helfen das zu erkennen“.

Sicher, der Satelliten-Hacking-Wettbewerb kann ein bisschen ein PR-Gag sein. Aber es ist einer mit praktischen Vorteilen. Es wird mindestens einen Satelliten sicherer und relevanter machen. Cooper vom Aviation Village sagt, dass der Weltraum zu einem so wichtigen Teil der Cybersicherheit von Flugzeugen geworden ist, dass das Aviation Village im nächsten Jahr das Aerospace Village sein wird.

Und wenn Satelliten nicht dein Ding sind? Mach dir keine Sorgen. Roper sagt, er tue sein Bestes, um ein ganzes Flugzeug für Hacks zur Defcon 2021 zu bringen. Sie haben nur ein paar Probleme einen Platz zu finden.

Nachtrag des Autors

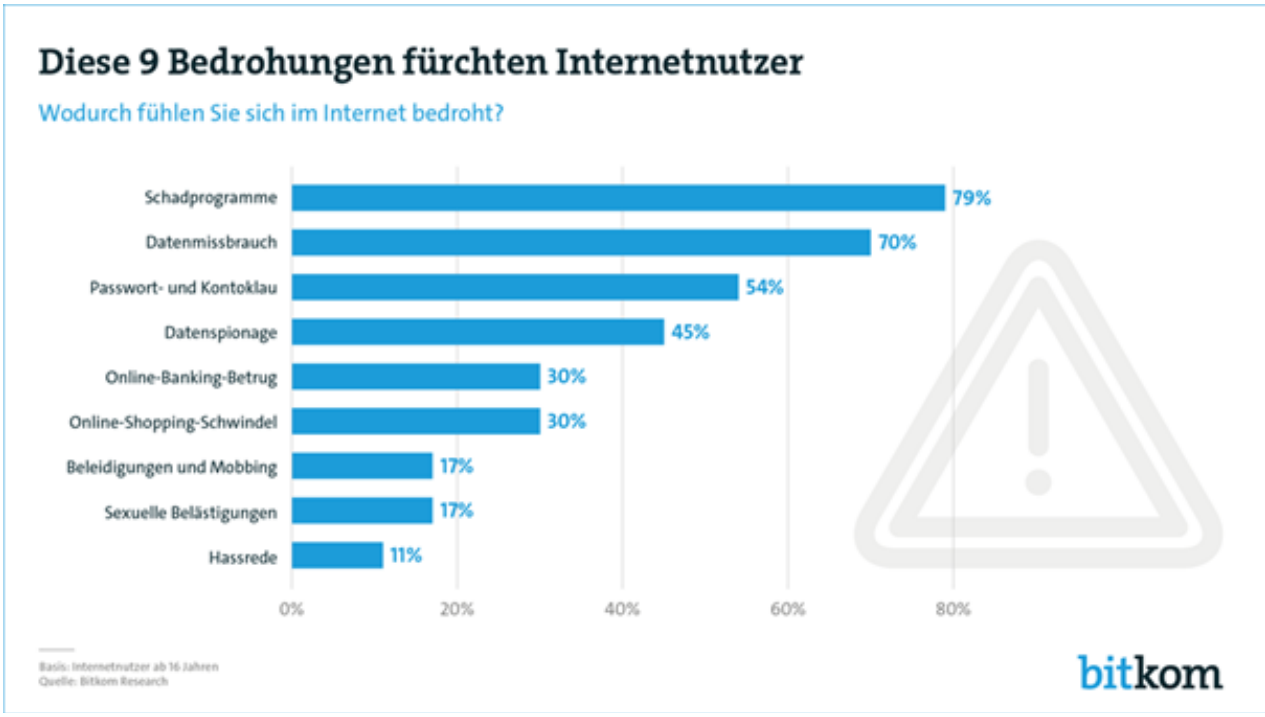
Im Jahre 2002 waren die ersten Anzeichen eines Krieges der USA gegen den Irak sehr deutlich. Zu dieser Zeit glaubte die Welt dass Machthaber Saddam Hussein kurz vor der Fertigstellung einer eigenen Atombombe stand. Auch der Autor glaubte das. So schrieb er dann Ende 2002 eine Story in der Fachzeitschrift „Tele-Satellit“, wie der Irak ohne Menschleben zu gefährden und deutlich billiger die US-Amerikaner das Kriegsleben schwer machen könnte. Einfach einen starken Sender (im Megawattbereich) für rund 300 MHz bauen und ein FM-Signal auf den US Kommandosatelliten UHF Follow On (UFO) „schießen“. Nach dem System der korrespondierenden Gefäße würde das FM-Signal nicht nur einen Kanal dichtmachen, sondern gleich den ganzen Satelliten. Die Kommunikation der Amerikaner in dieser Region wäre mehr als nur empfindlich gestört. Das wäre billig und effektiv. Im März 2003 begann dann der Krieg. Fast zur gleichen Zeit traf der Autor in Dubai Saddams ehemaligen Atomminister Dr. Jafar al Jafar, der aus dem Irak geflohen war. In einem längeren Gespräch erklärte er, dass das Atomwaffenprogramm schon Jahre vorher im Anfangsstadium auf Eis gelegt wurde. Ja, Saddam Hussein wusste von der Story des Autors, da auch an die Regierung in Bagdad die arabische Ausgabe der Zeitschrift ging. Zumindest sorgte der Inhalt der Geschichte für Gelächter in der Morgenrunde der Minister. Heute wissen wir, dass dieser Krieg durch eine Lüge der USA entstand. Einen solchen Satelliten durch die Defcon-Hacker zu kapern dürfte kein Problem sein, da die Schwachstellen der UFO-Satelliten noch existent sind. Der Autor wurde leider nicht eingeladen.

INTERNET

Internetnutzer fürchten diese 9 Bedrohungen

Von Schadprogrammen bis Hassrede

Bitkom gibt Sicherheitstipps



Die überwiegende Mehrheit der Internetnutzer fühlt sich von Cyberkriminalität bedroht.

Diese neun Vorfälle fürchten sie am meisten:

1. Schadprogramme

Bösartige Programme auf dem Computer oder Smartphone wie Viren oder Trojaner – für acht von zehn Internetnutzern (79 Prozent) ist dieses Szenario eine Bedrohung.

2. Datenmissbrauch

Der Datenschutz wird nicht eingehalten, persönliche Daten unerlaubt weitergegeben und z.B. für Werbung missbraucht: Sieben von zehn Onlinern (70 Prozent) fühlen sich dadurch bedroht.

3. Passwort- und Kontoklau

Cyberkriminelle können zu schwache Passwörter ausnutzen und fremde Online-Konten übernehmen. Für mehr als jeden zweiten Internetnutzer (54 Prozent) ist diese Vorstellung bedrohlich.

4. Datenspionage

Wenn der Staat mitliest: Geheimdienste greifen auf verschlüsselte oder persönliche Kommunikation zu – 45 Prozent der Onliner haben Sorge davor.

5. Online-Banking-Betrug

Fremder Zugriff auf die eigenen Finanzen: Betrug beim Online-Banking sehen drei von zehn (30 Prozent) als Bedrohung.

6. Online-Shopping-Schwindel

Die Ware ist bestellt oder ersteigert worden, das Geld ist überwiesen, doch die Lieferung kommt niemals an: Davor fürchten sich ebenfalls 30 Prozent der Internetnutzer.

7. Beleidigungen und Mobbing

Diskussionen in sozialen Netzwerken oder Online-Foren lassen

zuweilen einen guten Ton vermissen. Nicht selten sind Onliner auch mit Beleidigungen oder gar gezieltem Mobbing konfrontiert. Mehr als jeder Sechste (17 Prozent) empfindet dies als bedrohlich.

8. Sexuelle Belästigungen

Gezieltes Ansprechen von Personen, um sexuelle Kontakte anzubahnen – das sogenannte Cyber-Grooming ist nur eine Form von sexueller Belästigung im Internet. 17 Prozent der Onliner fühlen sich dadurch bedroht.

9. Hassrede

Hassbotschaften und Volksverhetzung sind auch im Internet ein Problem. Jeder neunte Onliner (11 Prozent) sieht darin für sich eine Bedrohung.

Schutz vor Cyberkriminellen

Wie sich Nutzer vor Cyberkriminellen schützen können, hat Bitkom in 6 Tipps zusammengestellt. Weitere Informationsangebote zum Thema Sicherheit im Internet bieten auch Initiativen wie Deutschland sicher im Netz.

Hinweis zur Methodik: Grundlage der Angaben ist eine repräsentative Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.004 Internetnutzer ab 16 Jahren telefonisch befragt. Die Umfrage ist repräsentativ. Die Fragestellung lautete: „Wodurch fühlen Sie sich im Internet bedroht?“

6 Tipps für die IT-Sicherheit

bitkom

Komplexe Passwörter nutzen

Das Passwort sollte mindestens acht Zeichen lang sein und sowohl Groß- und Kleinbuchstaben als auch Ziffern und Sonderzeichen enthalten. Das Passwort sollte kein Begriff sein, der sich im Wörterbuch finden lässt. Außerdem sollte es keinen Bezug zum beruflichen oder privaten Umfeld haben: Weder Geburtsdaten, noch Lieblingsromane oder Namen der Kinder sind sichere Passwörter.

Passwort-Manager als Kennwort-Tresor einsetzen

Für unterschiedliche Dienste sollte man auch unterschiedliche Passwörter nutzen. Passwort-Manager generieren komplexe Passwörter und heben diese sicher auf. Merken muss man sich nur noch ein Generalpasswort.

Mehr-Faktor-Authentifizierung nutzen

Wird die Zwei-Faktor-Authentifizierung angeboten, sollte man sie nutzen: Beim Einloggen gibt man sein Passwort ein. Daraufhin bekommt man eine TAN per SMS. Nur wenn sowohl das Passwort als auch die TAN stimmen, wird man eingeloggt.

Regelmäßig Updates fahren

Sicherheitslücken sind meist Programmierfehler, durch die sich Viren und Schadsoftware Zugang zu den Daten verschaffen. Sicherheitsupdates schließen diese Lücken. Deshalb sollte man sie schnellstmöglich installieren. Wenn Programme Updates automatisch einspielen können, sollte man das in den Einstellungen aktivieren.

Vorsicht bei dubiosen Mails und Anfragen

Oberstes Gebot: den gesunden Menschenverstand nutzen. Banken und andere Unternehmen bitten ihre Kunden nie per E-Mail, vertrauliche Daten im Netz einzugeben. Diese Mails sind am besten sofort zu löschen. Das Gleiche gilt für E-Mails mit unbekanntem Dateianhang oder verdächtigen Anfragen in sozialen Netzwerken.

Informationen ernst nehmen und handeln

Wenn über Sicherheitslücken, Hacks oder ähnliche Vorfälle berichtet wird, sollten Nutzer handeln. Um an Informationen zu kommen, können Nutzer beispielsweise Apps wie das Sicherheitsbarometer von DSIN einsetzen. Wichtig ist: aktiv werden! Sicherheit lebt vom Mitwirken alle

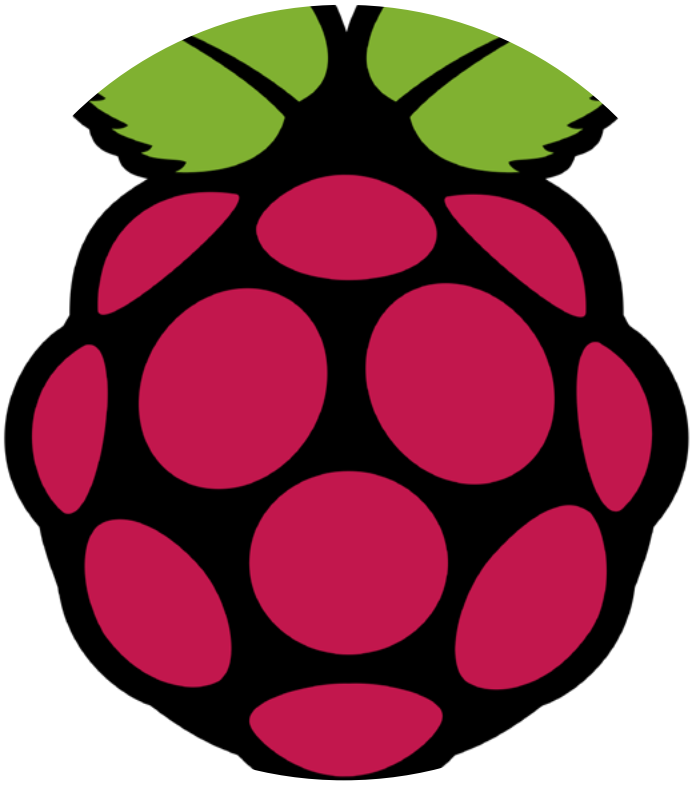
Quelle: BITKOM

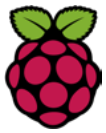
Demnächst NEU bei TecTime:

TecT.....

Vier aktuelle Raspberry-Pi-Alternativen

Einplatinenrechner im Vergleich





Der Raspberry Pi ist fast zum Synonym für Einplatinenrechner geworden.

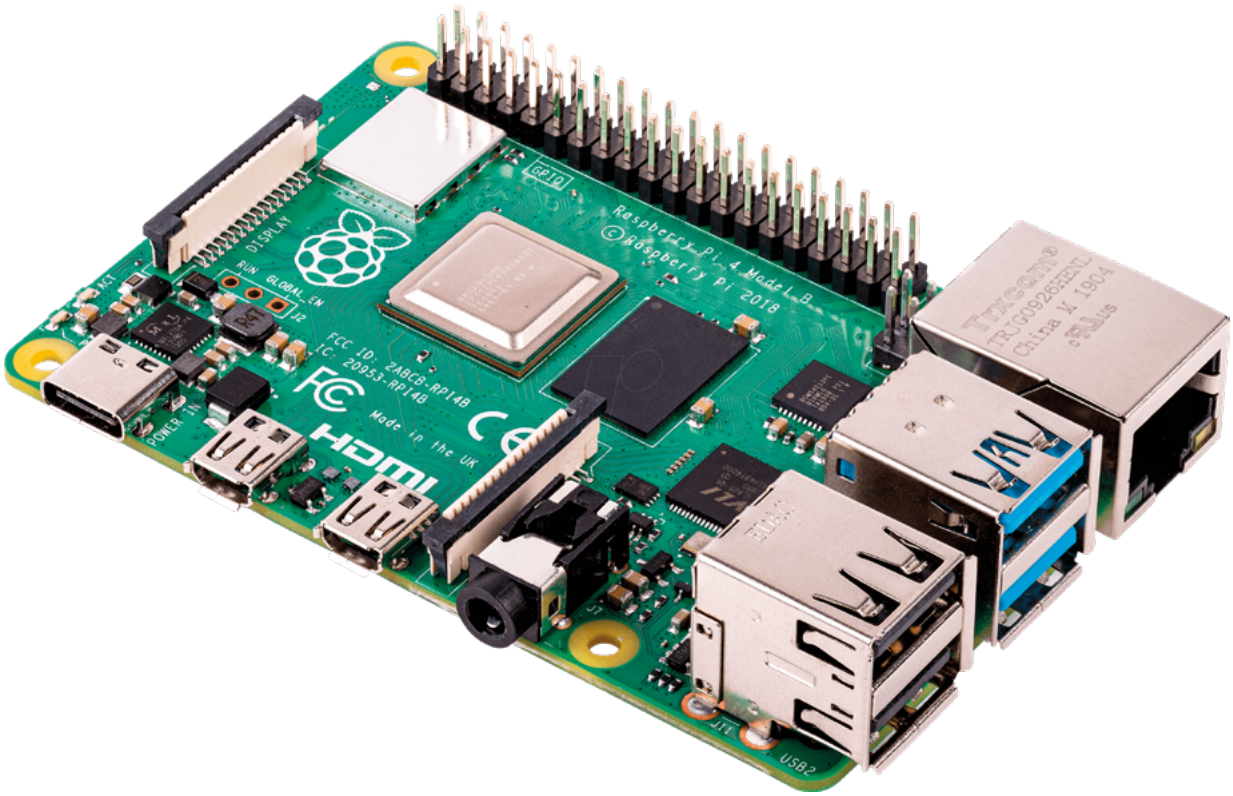
Der Mini-Computer im Kreditkartenformat eignet sich für unzählige Einsatzzwecke und ist schnell zum heiligen Gral der Bastlerszene geworden: Er kann z. B. als Web- oder Mailserver, aber auch als Grundlage für eine ownCloud dienen, lässt sich als Mediacenter einrichten oder zu einer Spielkonsole umfunktionieren.

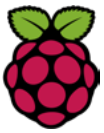
Die Möglichkeiten sind ebenso vielfältig, wie der Preis niedrig ist – viele Ausführungen sind für unter 40 Euro zu bekommen.

Doch es gibt auch noch kleinere, leistungsstärkere oder günstigere Alternativen zum Raspberry Pi.

Ein Überblick.

Die aktuelle Vorlage:
Der Raspberry Pi 3 Modell B

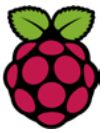


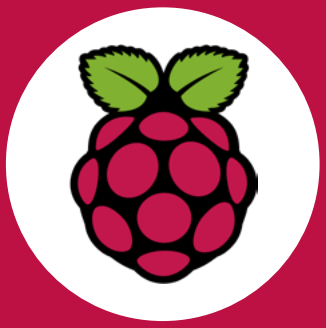


Inzwischen gibt es den Raspberry Pi in verschiedenen Versionen. Als Grundlage für den Vergleich mit den Alternativen dient uns der aktuelle Raspberry Pi 3 Modell B. Er ähnelt den Vormodellen zwar optisch, bietet aber einige neue Features – freilich ohne dabei seine Grundkonstruktion zu verändern. So gibt es mit dem Quadcore-Prozessor Cortex-A53 erstmals 64-bit. Der Chip taktet mit bis zu 1,2 GHz. Wie auch bei den Vorgängern gibt es mit dem Raspberry Pi 3 wieder 1 GB Arbeitsspeicher. In Sachen Konnektivität hat sich jedoch einiges verbessert: So sind erstmals WLAN und Bluetooth mit an Bord. Das Mehr an Power hat allerdings eine Kehrseite: Denn der Strombedarf hat sich im Vergleich zu den vorigen Versionen leicht erhöht. Das dürfte allerdings nur im Server-Dauerbetrieb ins Gewicht fallen.

Anschlussmöglichkeiten für Zubehör aller Art sind dafür immer noch in Hülle und Fülle vorhanden: So sorgen vier USB-2.0-Buchsen für erstaunlich viele Anbindungsgelegenheiten. Ein LAN-Anschluss ist ebenso wieder verfügbar wie eine sogenannte Pinleiste für Spezialzubehör. Hier stehen 40 GPIO-Pins zur Verfügung. Als Video- und Sound-Schnittstelle gibt es einen HDMI-Anschluss. Für die analoge Soundausgabe ist zudem ein 3,5-mm-Klinkenstecker auf dem Mini-Computer untergebracht.

Ebenso vielfältig sind die denkbaren Software-Lösungen: Neben den bereits zuvor möglichen Betriebssystemen auf Linux-Basis (NOOBS, Raspbian u. a.) und ersten Android-Gehversuchen wird wie beim Raspberry Pi 3 Modell B auch Windows 10 IoT Core unterstützt. Dabei handelt es sich nicht um ein klassisches Windows-System, sondern um ein spezielles Entwickler-Betriebssystem. IoT leitet sich dabei von „Internet of Things“ (Internet der Dinge) ab. Preislich liegt der Raspberry Pi 3 bei rund 40 Euro.

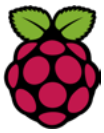




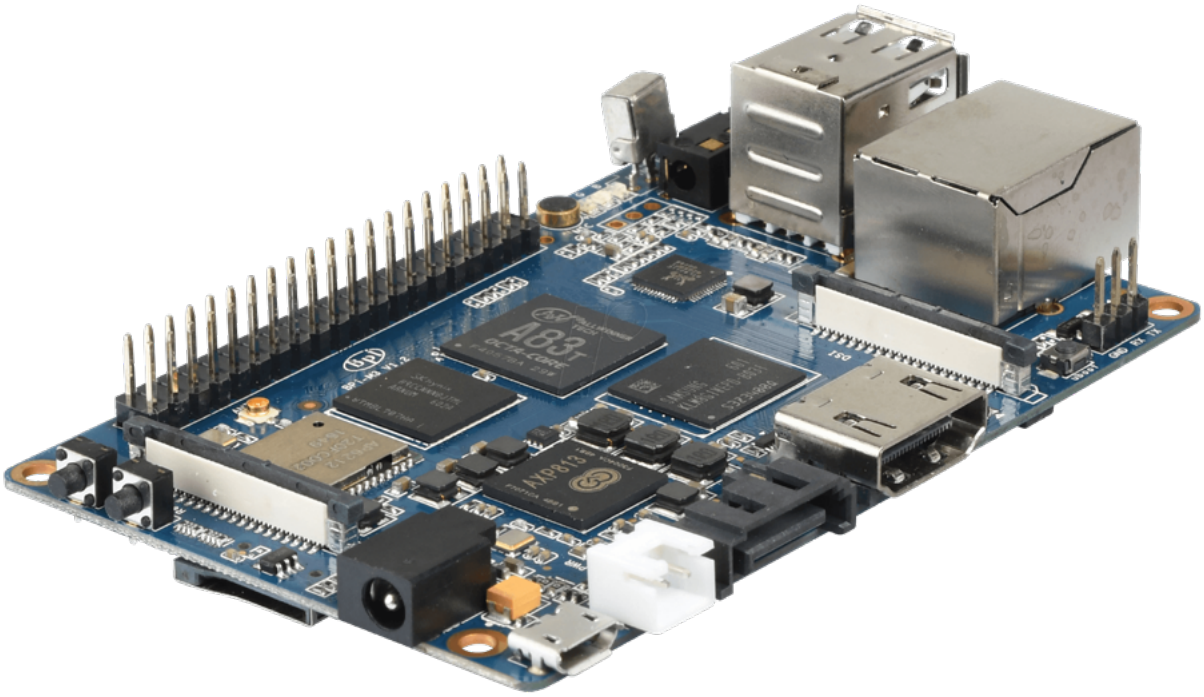
Welche Raspberry-Pi-Alternativen gibt es?

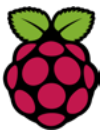
Die Vielfalt an guten Raspberry-Pi-Alternativen ist groß – so groß, dass in diesem Artikel eine Auswahl getroffen werden muss.

Die Hersteller setzen zudem unterschiedliche Schwerpunkte, was einen Vergleich nicht mit allen Alternativen sinnvoll macht. Vorgestellt werden sollen daher nur aktuelle Single Board Computer (SBC), die sich preislich in direkter Nachbarschaft zum Raspberry Pi befinden oder das große Vorbild besonders herausfordern:
*Der ähnlich klingende **Banana Pi M3**,*
*der extrem günstige **C.H.I.P.***
*sowie das leistungsstarke **Cubieboard5***
*und der exotische **NanoPi M3**.*



Banana Pi M3



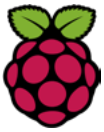


Der durchschlagende Erfolg und Einfluss des Vorbilds schlägt sich auch auf die Benennung dieser Raspberry-Pi-Alternative nieder. Der Banana Pi ist aber mehr als nur eine bloße Kopie des namhaften Vorbilds – denn die kleine Wunderkiste hat einiges auf dem Kasten: Mit dem starken Allwinner-A83T-Prozessor inklusive acht ARM-Cortex-A7-Kernen und einer maximalen Taktung von 1,8 GHz ist zumindest auf dem Papier für ordentlich Power gesorgt. Auch der Arbeitsspeicher ist mit 2 GB doppelt so hoch wie beim unmittelbaren Konkurrenten.

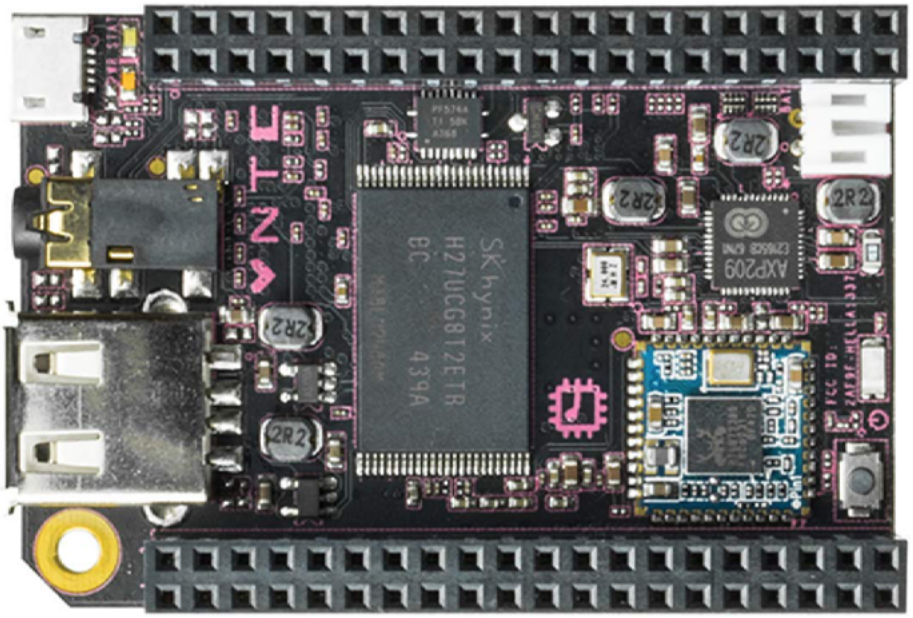
Breit aufgestellt ist der Banana Pi auch mit Anschlussmöglichkeiten: So gibt es neben einem HDMI-Anschluss auch einen 3,5 mm Klinkenstecker für die Tonausgabe, einen DSI-Display- und CSI-Kameraanschluss sowie einen integrierten Infrarot-Empfänger – und sogar ein On-Board-Mikrofon für unkomplizierte Tonaufnahmen ist verbaut. Abstriche gibt es bei dieser Raspberry-Pi-Alternative allerdings bei den verfügbaren USB-Ports: So wurden lediglich 2 USB-2.0-Hosts verbaut – halb so viele wie beim Raspberry Pi 3. Dafür fährt der Banana Pi M3 ebenfalls mit On-Board-WLAN und -Bluetooth und einer 10/100/1.000-Mbit-Ethernet-Netzwerkschnittstelle auf. Vor allem der SATA-Anschluss zeichnet den Banana Pi im Vergleich mit dem Raspberry Pi aus: Wurde dieser noch beim unmittelbaren Vorgänger, dem Banana Pi M2, eingespart, können mit dem M3 wieder unproblematisch Festplatten angeschlossen werden. Zudem stehen auch ein Micro-SD-Karten-Slot und ein 8 GB umfassendes eMMC-Modul zur Verfügung.

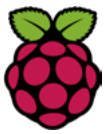
Laut Herstellerangaben können auf dem Banana Pi M3 ebenfalls ein Großteil der gängigen Betriebssysteme für Einplatinencomputer installiert werden – darunter verschiedene Linux-Derivate oder Android.

Ob sich der Banana Pi M3 wirklich als Raspberry-Pi-Alternative eignet, entscheidet nicht zuletzt der Preis: Mit rund 90 Euro schlägt er mehr als doppelt so kräftig zu Buche wie der große Konkurrent. Letztlich eine logische Konsequenz der leistungsstärkeren Technik: Mehr kostet schließlich mehr. Gerade Einsteiger fahren in der Regel mit dem Raspberry Pi dennoch besser – die große Community und die einsteigerfreundlichen Standard-Betriebssysteme machen die Technik leichter zugänglich. Erfahrenere Bastler könnten sich dafür über die satte Leistung des Banana Pi M3 freuen.



C.H.I.P.



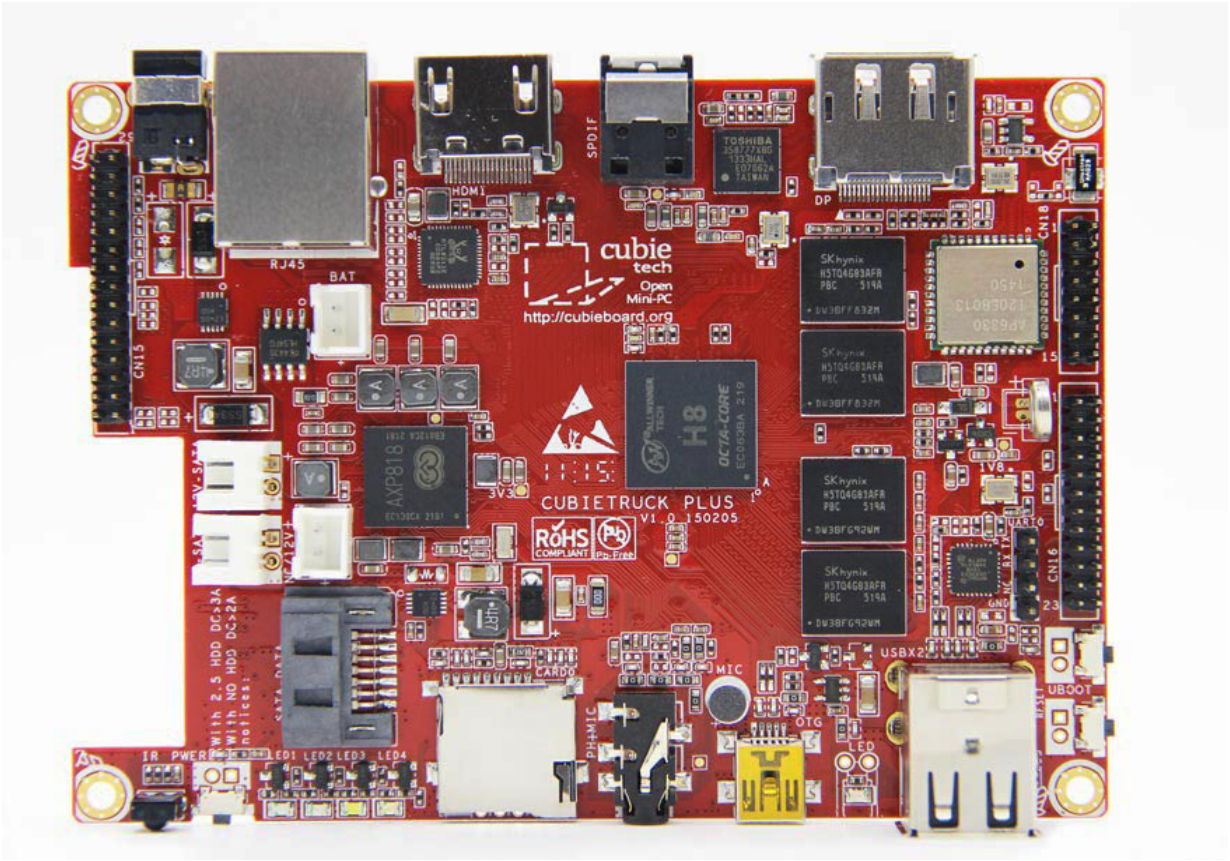


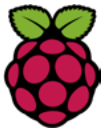
Der Preis des Raspberry Pi ist eine Ansage – doch der Single Board Computer C.H.I.P. weiß sie gekonnt zu erwidern: Mit einem Preis von gerade einmal 9 US-Dollar (rund 8 Euro) ist die kleine Maschine günstiger als alle anderen Alternativen zum Raspberry Pi. Ebenso deutlich unterboten wird die Größe des Raspberry Pi: Der von dem Start-up „Next Thing Co." entwickelte C.H.I.P. ist gerade einmal so groß wie eine Streichholzschachtel und mit 40 x 60 mm der kleinste in diesem Vergleich. Kein Wunder, dass das als Kickstarter-Projekt begonnene Vorhaben sofort seine Fans und Förderer fand: Innerhalb von nur 24 Stunden gingen bei den Entwicklern satte 200.000 US-Dollar zur Unterstützung des Projekts ein.

Abstriche gibt es zwangsläufig bei der Ausstattung: So verfügt C.H.I.P. lediglich über einen ARM-Cortex-R8-Single-Core-Prozessor mit einer Taktung von 1 GHz. Mit 512 GB RAM steht auch nur halb so viel Arbeitsspeicher zur Verfügung wie beim Raspberry Pi 3. Dafür gibt es WLAN- und Bluetooth-Schnittstellen und 4 GB Flash-Speicher, auf dem standardmäßig bereits die Linux-Distribution Debian vorinstalliert ist. So ist C.H.I.P. durchaus auch für Einsteiger eine gute Raspberry-Pi-Alternative – es kann sofort und ohne größere Umwege losgelegt werden. Allerdings ist lediglich ein Analog-Ausgang für Displays vorhanden. Für den Anschluss eines Bildschirms via HDMI oder VGA ist ein separater Adapter nötig. Rechnet man die Kosten für dieses Zubehör ein, bewegt man sich fast schon wieder in den Gefilden der leistungsstärkeren Konkurrenz.

Die Stromversorgung geschieht über einen Micro-USB-Port. Alternativ steht auch eine Lithium-Ionen-Batterie zur Verfügung. Damit kann der Mini-Computer auch sehr gut mobil genutzt werden. Kein Wunder, dass der Hersteller inzwischen auch einen portablen Ableger, den sogenannten Pocket C.H.I.P., auf den Markt gebracht hat. Das Gerät verfügt über einen integrierten Akku, der rund 5 Stunden halten soll. Allerdings ist die Taschenversion in erster Linie als mobile Spielkonsole konzipiert. Als tragbaren Mini-Linux-Computer kann man ihn dennoch verwenden, zumal auch die Pocket-Ausführung zum Modifizieren geeignet ist – auf der Herstellerseite wird sogar explizit dazu aufgerufen.

Cubieboard5/Cubietruck Plus

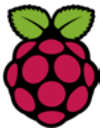




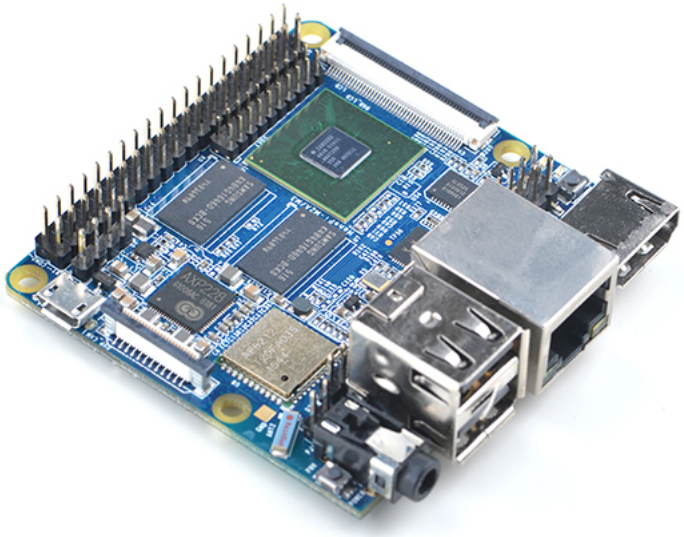
Einen ganz anderen Weg schlägt demgegenüber diese Raspberry-Pi-Alternative ein: Das Cubieboard5, das auch Cubietruck Plus genannt wird, legt seinen Schwerpunkt auf Leistung. Preislich liegt es – verglichen mit den vorigen Einplatinencomputern – deutlich am oberen Ende: Rund 100 Euro sind für den Mini-Computer hierzulande fällig. Herzstück des Boards ist ein Allwinner-H8-Prozessor, dessen acht Cortex-A7-Kerne sich auf maximal 2 GHz takten lassen. Als GPU-Kern wurde ein PowerVR SGX544 verbaut, und beim Arbeitsspeicher zieht das Cubieboard5 mit dem Banana Pi M3 dank großzügiger 2 GB gleich.

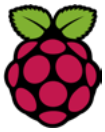
Zudem zeichnet sich das Cubieboard5 durch viele Anschlüsse aus: Auch hier ist standardmäßig WLAN mit an Bord – ebenso wie eine Bluetooth-Schnittstelle und ein LAN-Anschluss. Neben einem Micro-SD-Slot besteht zudem die Möglichkeit, HDD- oder SSD-Festplatten über den SATA-II-Anschluss mit dem Board zu verbinden. Für die Videoausgabe sind sowohl eine HDMI-1.4a-Schnittstelle wie auch Displayport 1.1 auf dem Cubieboard5 untergebracht. Auch ein 3,5-mm-Audioausgang ist verbaut. Bastler können sich dank 70 frei belegbarer Pins richtig austoben und zahlreiche externe Geräte an das Cubieboard5 koppeln. Dank einer festverbauten Lithium-Ionen-Batterie lässt sich das Cubieboard5 sogar kurzzeitig ohne Stromzufuhr betreiben, was es besonders für den Serverbetrieb interessant macht. Dank dieser Energiereserve lassen sich kurzzeitige Stromausfälle überbrücken und ein dadurch resultierender Datenverlust ggf. vermeiden.

Als Betriebssystem für diese Raspberry-Pi-Alternative können Herstellerangaben zufolge Android, Ubuntu „und viele andere Open-Source-Distributionen“ verwendet werden. Wie sich die einzelnen Betriebssysteme mit der Hardware vertragen, muss allerdings im Einzelfall ausprobiert werden.



NanoPi M3

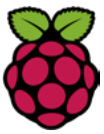




Das Beste aus beiden Welten – günstiger Preis bei satter Ausstattung – will die exotische NanoPi-Reihe des chinesischen Herstellers FriendlyARM vereinen: Die aktuellen Ausführungen – vom NanoPi Neo bis zum NanoPi M3 – wollen dezidiert als jeweilige Alternativen zu Raspberry-Pi-Modellen auftreten. Während der NanoPi Neo der kleinste unter den Einplatinencomputern von FriendlyARM und am ehesten mit dem Raspberry Pi Zero zu vergleichen ist, tritt der NanoPi M3 in Konkurrenz zum Raspberry Pi 3. Dabei schafft er es – trotz einer beachtlichen Ausstattung –, immer noch kleiner als der große Konkurrent zu sein: Der NanoPi M3 misst gerade einmal 64 x 60 mm, während der Raspberry Pi 3 wie sein unmittelbarer Vorgänger 93 x 63,5 mm groß ist.

An der Ausstattung ist trotzdem nicht gespart worden: Als Prozessor wurde ein Samsung S5P 6418 mit acht Cortex-A9-Kernen verbaut, die sich jeweils bis 1,4 GHz takten lassen. Auch beim Arbeitsspeicher zieht der NanoPi M3 mit 1 GB gleich und stellt somit eine gute Raspberry-Pi-Alternative dar. Zudem gibt es Anschlüsse in Hülle und Fülle: Ein Micro-SD-Karten-Slot, vier USB-2.0-Anschlüsse, ein MicroUSB-Port – etwa für die Stromversorgung – sowie jeweils ein HDMI- und 3,5-mm-Klinkenanschluss sind ebenfalls auf der winzigen Platine untergebracht. Auch die Anzahl der GPIO-Pins unterscheidet sich nicht vom großen Vorbild und beläuft sich auf 40 Stück.

Maus und Tastatur können über die Bluetooth-Schnittstelle angebunden werden, und eine Internetverbindung ist entweder via WLAN oder über den Ethernet-Port hergestellt. Softwareseitig lassen sich auf dieser Raspberry-Pi-Alternative wahlweise Android, Debian oder der Bootloader U-Boot ausführen. Die Dokumentation über das Wiki des Herstellers ist ausführlich. Ob sich allerdings um Exoten wie die NanoPi-Modelle eine ähnlich große Community mit herstellerunabhängigen Hilfestellungen aufbauen kann, bleibt noch abzuwarten. In Deutschland ist das Gerät aktuell noch nicht verfügbar. Online kostet der NanoPi M3 ca. 35 US-Dollar.



Fazit

Welche nun die besten Raspberry-Pi-Alternativen sind, hängt von vielen Faktoren ab – vor allem aber vom Einsatzzweck und dem Kenntnisstand des Nutzers. Wer einen reinen Datenserver betreiben möchte, kann auch zu schwächeren, dafür günstigeren und bestenfalls stromsparenderen Raspberry-Pi-Alternativen greifen. In diese Kategorie fällt beispielsweise der C.H.I.P.-Mini-Computer von Next Thing Co. Soll ein Mediaserver eingerichtet werden, ist ein HDMI-Anschluss heutzutage fast schon ein Muss. Ebenso wichtig ist in diesem Fall eine möglichst potente Hardware. Hierzu können sich erfahrene Nutzer beispielsweise das Cubieboard5 näher anschauen.

Nicht zu vernachlässigen ist aber auch die Software-Seite: Nur wenn ausreichend Software unterstützt wird, kann die Hardware überhaupt ihr volles Potenzial ausschöpfen. Gerade in dieser Hinsicht erweist sich der Raspberry Pi – besonders für Einsteiger – immer noch als perfekter Allrounder. Eine große Community bietet darüber hinaus Anregungen und Hilfestellungen. Allerdings stellen ebenso preiswerte oder nur wenig teurere Alternativen zum Raspberry Pi sogar eine überlegene Hardware zur Verfügung. Erfahrenere Nutzer finden etwa mit dem Banana Pi M3 oder dem Cubieboard5 leistungsstarke Alternativen – müssen aber beachten, dass u. U. nicht jede Software und Hardware ohne Weiteres unterstützt wird.

Malachit-DSP

Ein 177 Euro russischer tragbarer Breitband-SDR-Empfänger mit Touchscreen

Lange gewartet, doch nun ist er da. Und er kommt aus Russland. Der Malachite-DSP ist ein "all-in-one" tragbares SDR, das über einen Touchscreen und zwei Bedienknöpfe gesteuert wird. Der Empfänger deckt 0,1 MHz bis 1000 MHz mit einer Bandbreite von bis zu 160 kHz ab und die Individualsoftware unterstützt alle gängigen Modulationsarten. Das Gerät verbraucht 300mA und wird von einer Li-Ionen-Zelle versorgt. Es wird als moderner DEGEN- und TECSUN-Ersatz vermarktet, so dass es sich offenbar an den HF-Kurzwellenhörer (SWL) richtet.

Die produzierte Stückzahl scheint niedrig zu sein. Der Verkauf erfolgt derzeit über RX9CIM, einen der Projektentwickler. Die Kosten für eine komplett montierte Einheit betragen 12500 russische Rubel, das sind 177 Euro (ohne internationalen Versand). Man kann auch nur die Leiterplatte ohne Komponenten für 1100 Rubel (15,60 Euro) kaufen. Achtung: es gibt inzwischen Anbieter, die den Malachit-DSP angeblich liefern können, jedoch nur das Geld abkassieren und das war`s dann. Die einzige legitime Bestelladresse ist: malahit_sdr@rambler.ru.

Aus der Komponentenliste können wir ersehen, dass dieser SDR auf dem MSI001 Tunerchip läuft, der derselbe Tunerchip ist, der in der SDRplay Gerätefamilie verwendet wird. Im Gegensatz zu den SDRplay-Geräten, die einen Breitband-ADC MSi2500 verwenden, verwendet der Malachite-DSP jedoch einen Audio-Chip als RF-ADC. Dadurch entsteht ein 16-Bit-ADC, was zu einem hohen Dynamikbereich führt, jedoch auf Kosten der verfügbaren Bandbreite von nur 160 kHz. Ein STM32H743VIT6 mit ARM Cortex A7 Prozessor läuft auf einer scheinbar kundenspezifischen DSP- und GUI-Software. Die Software scheint DRM nicht zu unterstützen, aber die Modis AM, WFM, NFM, LSB, USB werden alle unterstützt.

Die Projektentwickler sind die Funkamateure RX9CIM George, R6DAN Vladimir und R6DCY Vadim.

Technische Daten

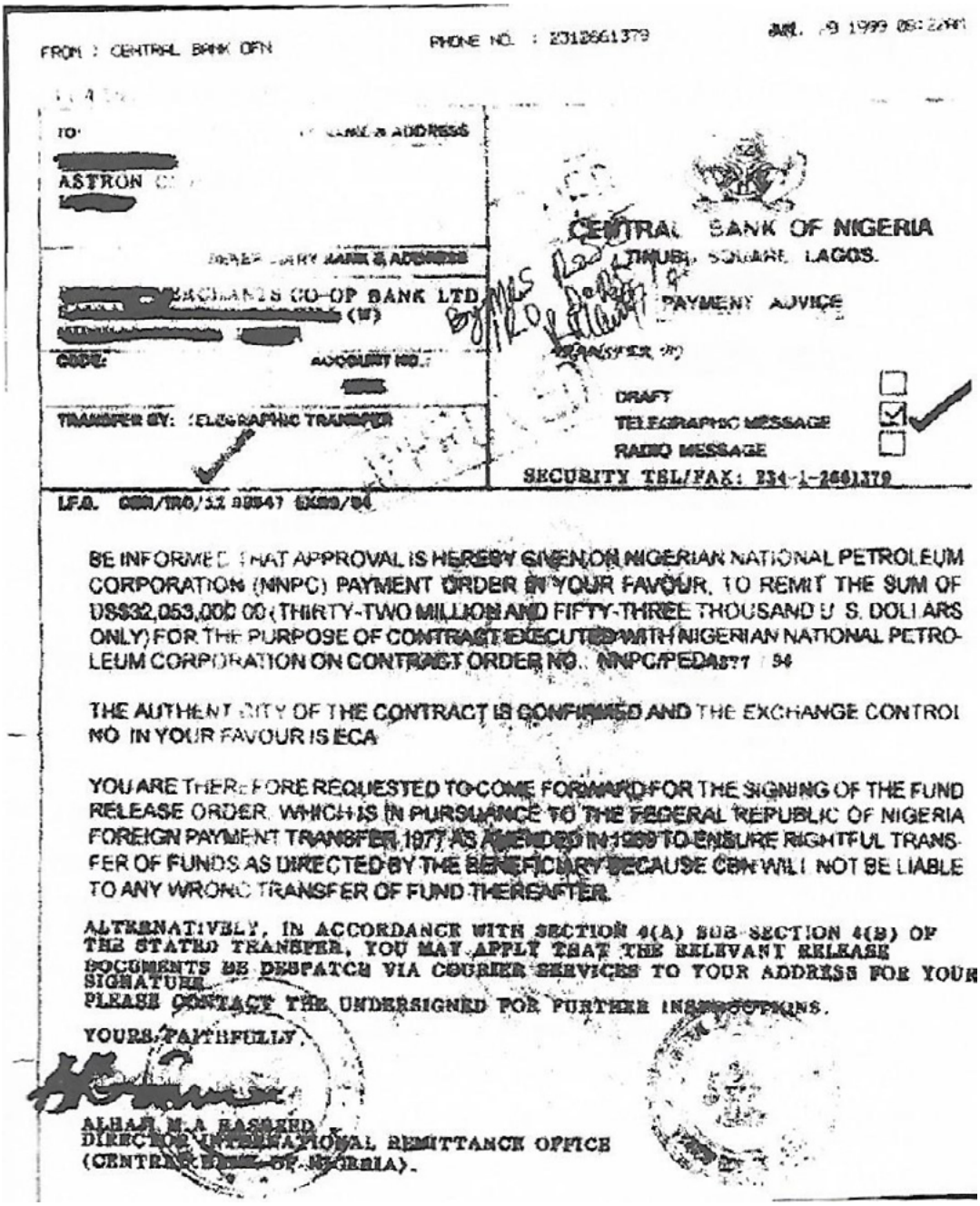
- 1 MHz bis 1000 MHz.
- Bandbreite 160 kHz.
- Modulationsarten AM, WFM, NFM, LSB, USB.
- Stromversorgung: Lithium-Ionen-Zelle.
- Verbrauch bis zu 300 mA

- Hauptchip ARM STM32H743VIT6 MCU Hochleistungs- und DSP mit DP-FPU
- ARM Cortex-M7 MCU mit 2MBytes Flash, 1MB RAM, 400 MHz CPU
- Die Leiterplatte wird aus vier Schichten gefertigt

Das YouTube Video zum Gerät kann unter https://youtu.be/BeyAX3jv_LM abgerufen werden. Bitte sicherstellen, dass die Untertitel für die automatische Übersetzung aktiviert sind.

Der Malachite-DSP erinnert uns ein wenig an den unveröffentlichten PantronX Titus II SDR, der als kostengünstig galt (mit einem Ziel von weniger als 100 Euro). Ein 100 kHz - 2 GHz Tablet-screen-basierter SDR, der den DRM-Empfang populärer machen sollte. Allerdings ist die Titus II-Hardware seit den ersten Nachrichten im Jahr 2016 nie produziert worden und scheint derzeit ein totes Projekt zu sein.

Vor 21 Jahren



FROM : CENTRAL BANK OFN PHONE NO. : 2312661379 JAN. 19 1999

TO:
[redacted]
ASTRON
[redacted]

BENEFICIARY BANK & ADDRESS
[redacted] BACHANAS CO-OP BANK LTD (M)
[redacted]
CODE: ACCOUNT NO.:
[redacted]
TRANSFER BY: TELEGRAPHIC TRANSFER

CENTRAL BANK OF NIGERIA
TINUBU SQUARE LAGOS.
PAYMENT ADVICE
TRANSFER NO.
DRAFT
TELEGRAPHIC MESSAGE
RADIO MESSAGE
SECURITY TEL/FAX: 234-1-2661379

L.P.O. CBN/TRO/12 00547 EXCO/94

BE INFORMED THAT APPROVAL IS HEREBY GIVEN ON NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC) PAYMENT ORDER IN YOUR FAVOUR, TO REMIT THE SUM OF US$32,053,000.00 (THIRTY-TWO MILLION AND FIFTY-THREE THOUSAND U.S. DOLLARS ONLY) FOR THE PURPOSE OF CONTRACT EXECUTED WITH NIGERIAN NATIONAL PETROLEUM CORPORATION ON CONTRACT ORDER NO. NNPC/PEDA/577 94

THE AUTHENTICITY OF THE CONTRACT IS CONFIRMED AND THE EXCHANGE CONTROL NO IN YOUR FAVOUR IS ECA

YOU ARE THEREFORE REQUESTED TO COME FORWARD FOR THE SIGNING OF THE FUND RELEASE ORDER, WHICH IS IN PURSUANCE TO THE FEDERAL REPUBLIC OF NIGERIA FOREIGN PAYMENT TRANSFER, 1977 AS AMENDED IN 1999 TO ENSURE RIGHTFUL TRANSFER OF FUNDS AS DIRECTED BY THE BENEFICIARY BECAUSE CBN WILL NOT BE LIABLE TO ANY WRONG TRANSFER OF FUND THEREAFTER.

ALTERNATIVELY, IN ACCORDANCE WITH SECTION 4(A) SUB-SECTION 4(B) OF THE STATED TRANSFER, YOU MAY APPLY THAT THE RELEVANT RELEASE DOCUMENTS BE DESPATCH VIA COURIER SERVICES TO YOUR ADDRESS FOR YOUR SIGNATURE.
PLEASE CONTACT THE UNDERSIGNED FOR FURTHER INSTRUCTIONS.

YOURS FAITHFULLY

ALHAJI M.A BASHEER
DIRECTOR INTERNATIONAL REMITTANCE OFFICE
(CENTRAL BANK OF NIGERIA).

Angebliche Überweisung aus Nigeria

Ende 1998 erschien diese Story in der Fachzeitschrift „Tele-Satellit“ und sorgte für Nervosität bei den Tätern und brachte dem Autor eine Morddrohung ein.

Nigeria Connection

Im wohlverdienten Urlaub auf Redaktionskosten im firmeneigenen Iglu an der herrlichen Nordküste Grönlands erreichte mich die Kunde, dass sich nach relativ langer Ruhe die Scam-Mafia aus Nigeria wieder melden würde. Vor einigen Jahren in Teil neun dieser Serie wurde über die Machenschaften berichtet, und eigentlich bestand auch kein Grund mehr, sich darum zu kümmern, denn Staatschef Sani Abacha von Shells Gnaden war verschwunden, und nach fast demokratischen Wahlen war der zivile Machthaber Olusegua Obasanjo am Steuer. Und der hatte gleich versprochen, mit den Scam-Letter Betrügern und korrupten Beamten abzurechnen. Wie das mit „abrechnen" gemeint sein mag, wissen wir nicht. Fest steht jedoch, dass nach einer Schrecksekunde die alten Figuren — teilweise unter anderen Namen — wieder ihr Unwesen treiben.

Vorgesehen hatte ich eigentlich einen ersten Erfahrungsbericht mit dem neuen Ikonos-Satelliten der Space-Imaging Group. TSI berichtete als erste Fachzeitschrift weltweit bereits ausführlich über das Projekt, kommerzielle Fotos mit einer Auflösung von einem Meter anzubieten, und als Dank bekommt die TSI-Redaktion auch die ersten Bilder des Satelliten. Auch die eigene Empfangsanlage ist inzwischen fertiggestellt und wartet eigentlich nur auf die ersten Signale. Leider befand sich der Satellit zum Redaktionsschluss noch in seiner 90-Tage Testphase. Alles hatte sich im Lauf der Jahre verzögert. Einsprüche diverser Geheimdienste (vor allen Dingen aus Israel) und der verunglückte Start von Ikonos-l waren der Grund. Die Auflösung der Fotos könnte heute schon leicht unterhalb der Im-Grenze liegen, doch hier sprach die National Security Agency (NSA) in den USA ein Machtwort. Nicht ganz von sich aus, auch hier drückten die Israelis von hinten. So müssen sich die polizeilichen Organisationen, die sich mit Mord und Tot- schlag beschäftigen, noch etwas gedulden, um endlich Fotos in hoher Auflösung einer bestimmten geographischen Zone und von einem bestimmten Zeitpunkt zu bekommen.

Nur so lässt sich eventuell feststellen, ob zu einem Tatzeitpunkt z.B. ein Auto an einem Waldrand geparkt wurde und wie es denn ungefähr aussehen könnte. Immerhin lässt sich mit dem IKONOS schon mal die Farbe und die Größe bestimmen. Nach meinem Vorschlag und nach einem konkreten Fall lief in süddeutsches LKA in die geheimdienstliche Sackgasse. Aus Sicherheitsgründen wollte man nicht helfen, obwohl die Keyhole-Satelliten der Amerikaner hier Hilfe leisten könnten, ohne ihr Gesicht zu verlieren.

Scam-Mafia

In den letzten 15 Jahren sich unter verschiedenen Regierungen — von denen nicht nur geduldet — die Nigeria-Connection etabliert. Unter verschiedenen Absendern versehen mit falschen Briefköpfen irgendwelcher Ministerien — werden an (vermeintlich) wohlbetuchte Amerikaner und Europäer brandeilige Briefe, Faxe und neuerdings auch E-Mails geschickt. Darin („Privat/Confidential") wird dem Empfänger ein kleines Millionen-Geschäft vorgeschlagen. Ein Betrag (z.B. 20 Millionen US-Dollar) muss angeblich außer Landes geschafft werden. Der Grund könnten überschüssige Einnahmen aus dubiosen Ölgeschäften sein, die gewaschen werden müssen, oder in letzter Zeit angesammelte Gelder von Ministern, die sich im Ausland nach der Machtübernahme durch Zivilisten eine neue Existenz aufbauen wollen. Dazu benötigt man dringend ein unverfängliches Auslandskonto, und das sollte partout das des Briefempfängers ein. Man möge doch alle Bankverbindungen bekanntgeben, damit die 20 Millionen US Dollar überwiesen werden können.

Als kleine Anerkennung für die geleisteten Dienste dürfe der Empfänger auch gleich 20% (4 Millionen Dollar) für sich abzweigen. Nur schnell muss alles gehen, und ein Rückruf noch heute wäre äußerst wichtig. Wer dumm und geldgierig genug ist, fällt darauf rein. Eine Kontonummer ist schließlich kein Geheimnis, und die kann man ja mal mitteilen. Sollte diese Kontonummer erkennbar ein verstecktes Konto in Liechtenstein, der Schweiz oder auf den Antillen sein, wird es ernst. Sollte unser Mr. Raffgier die Restfunktionen seiner kleinen Walnuss im Kopf abgeschaltet haben und auch noch das Passwort seines Kontos nennen, kann er die Sache eigentlich gleich vergessen. Der nächste Kontoauszug wird einen Saldo von 0,00 ausweisen.

Erstes Angebot aus Nigeria

TTN: [redacted]

Subject: ATTN: [redacted]
Date: Thu, 2 Sep 1999 03:06:57 -0700 (PDT)
From: STEPHEN HOZANE <hozanests@yahoo.com>
To: [redacted]

NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC) FALOMO IKOYI, I.AGOS.

ROM: DESK OF: STEPHEN HOZANB (DR) .
E-MAIL: HOZANESTS@YAEOO.COM

ATTN: [redacted]

DEAR STR,

CONFIDENTIAL BUSINESS PROPOSAL

1 AM DIRECTOR OF NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC) WE ARE MAKING THIS CONTRACT WITH YOU BECAUSE OF THE RELIABLE INFORMATION. WE GATHERED FROM THE NIGERIAN CHAMBERS O? COMMERCE AND INDUSTRY HIGHLIGHTING YOUR COMPANY'S PROFIL. THE INEOPETION IS SO POSITIVE AS TO CONVINCE US THAT YOU WOULD BE CAPABLE OF PROVIDING US WITH SOLUTION TO A MONEY TRANSFER TRANSACTION OF SIXTY—FIVE MILLION, FIVE HUNDRED THOUSAND UNTIED STATES DOLLARS ONLY (US$65.5M) .

WE ARE EMBERS OF THE SPECIAL COMMITTEE FOR BUDGETS AND PLANNING cp THE MINISTRY OF THIS COi011TTEE IS PRINCIPALLY CONCERNED WITH CONTRACT APPRAISALS THE APPROVAL 0? CONTRACTS IN ORDER 0?
PRIORITIES AS REGARDS CAPITAL PROCECTS OF THE MILITARY GOVERNI.ENQ O?
NIGERIA. WITH OUR POSITIONS, WE EAVE SUCCESSFUL SECURED FOR OURSELVES
TEE SUM OF MILLION, ?IVE HUNDRED THOUSAND UNITED STATES DOLLARS ONLY (US$65.5M) THIS AMOUNT WAS ACCUMU%ATED THROUGH
UNDECLARED FROM SALES 0? CRUDE DURING THE GULF WAR.

Der Besitzer eines „anständigen" Kontos erhält ein tolles Transfer-Schreiben der Bank of Nigeria, in dem man ihm mitteilt, dass der erwartete Betrag zur Überweisung ansteht, jedoch noch einige Formalitäten nötig seien. Unter anderem stehen noch die Transfer-Kosten in Höhe von 1% der Summe (200.000 US-Dollar) aus. Der Auftraggeber sei bereit, die Hälfte davon selbst zu übernehmen, die andere Hälfte sollte jedoch schnellstens überwiesen werden. Reagiert der Empfänger zögerlich, so wird er mit tollen Schreiben und einigen kleinen Zusatzforderungen in Atem gehalten, bis ihm derselbe ausgeht. Unsere Scam-Letter Mafia hat ihr Ziel erreicht und ist von nun an nicht mehr erreichbar.

In Folge neun dieser Serie bewiesen wir, dass es selbst mit verhältnismäßig einfachen Mitteln und etwas Sachkenntnis möglich ist, den Telefon/Fax- Verkehr dieser Gangster via Satellit mitzuhören und zu lesen. Den Autor erreichten nach Veröffentlichung einige nette Einladungen nach Nigeria, die er allerdings dankend ablehnte.

Lauschangriff II

Nach entsprechenden Hinweisen auf neue Aktivitäten wurde das alte Equipment wieder aktiviert. Inzwischen funktionierte auch das provisorische Fax-Modem etwas besser. Zumindest waren die Texte zu 80% lesbar. Da ein überwiegender Teil internationaler Telekommunikation über die diversen Intelsats läuft, war es erst einmal wichtig, den richtigen Satelliten zu finden. Vor einigen Jahren war es die Position 60 0 Ost. Hier wird inzwischen ein Hemi-Beam eingesetzt, und der ist leider in den nördlicheren Gefilden nicht empfangbar. Auf Nachfrage stellte sich auch schnell heraus, DEAR dass die 600-Position zwar noch von der Bodenstation Lanlate I genutzt wird, doch überwiegend im innerafrikanischen Verkehr.
Die nächsten Tage verzog ich mit allen Antennen-Listings auf den Dachboden und kam erst nach diversen Drohungen seitens der Familie und des Verlegers mit Spinn- weben zwischen den Armen wieder runter. Immerhin mit einigem Erfolg. Es mussten die Positionen 27 und 24,5 0 West sein. Die restlichen Infos kamen von lieben Menschen auf der IBC99, die als Belohnung die der Presse zustehenden Verzehrbons bekamen.

Es klappte auf Anhieb. Lanlate-2 (LAN-02a) bedient mit FDM 24,5 0 West im C-Band und Lagos-4 (LAG-04B) versorgt 27,5 0 West mit analogem SCPC. FDM wird für Telefonie, Fax und Data von Telekommunikations-Organisationen genutzt; SCPC sehr oft von Sicherheitsdiensten, Hilfsorganisationen, Ölgesellschaften und wesentlich zweifelhafteren Diensten. Der FDM-Verkehr ist mit recht einfachen Mitteln zu verfolgen. Man nehme einen etwas größeren Spiegel für das C-Band (Minimum: 180cm), einen analogen Low-Threshold-Receiver und einen erstklassigen SSB-Radio-Empfänger, der den Frequenzbereich bis etwa zehn MHz überstreicht (NRD; ICOM, AOR oder militärische Surplus-Geräte). Der Baseband-Videoausgang des Sat-Receivers wird über Koaxialkabel auf dem kürzesten Weg mit dem Antenneneingang des Kurzwellen-Receivers verbunden. Im C-Band wird auf betimmten Satelliten, die FDM transportieren, nach Transpondern gesucht, die sich durch dunkle Störungen auf dem Kontrollmonitor bemerkbar machen. Dieses „Störsignal" ist nichts anderes als FDM. Der Empfang wird der Low-Threshold-Funktion optimiert. Firmen-Bierzelt für

Nun wird der nachgeschaltete KW-Receiver im Bereich von 0 bis ca. 4MHz auf dem Münchner sehr vorsichtig in USB und LSB (oberes und unteres Seitenband in SSB- Modus) durchsucht. Theoretisch gibt es alle 4kHz einen Kanal. Eine reine Lern- und Nervensache ist es nun, diese Radiosignale einer bestimmten geografischen Gegend zuzuweisen. Ein Receiver mit eingebautem DTMFModul (z.B. AR5000) kann die gewählten Telefonnummern mitlesen und vereinfacht die Suche natürlich. Nigeria hat den Landescode 234, und so filtert man nur diese Telefonate und Faxe aus.

Bitte nicht nachmachen, denn das ist in den meisten Ländern verboten und geschah auch in unserem Fall rein experimentell. Dies ist wiederum am Standort unserer Monitoranlage erlaubt.

Die nächsten Wochen konzentrierte ich mich auf 24,5 0 West und vergaß meine Kollegen, die Sich auf Einladung des Verlegers mit mitgebrachtem Firmen-Bierzelt für zehn Personen und Bier aus dem lokalen Supermarkt auf dem Münchner Oktoberfest vergnügten. Und das alles auf Verlegerkosten.

Doch es lohnte sich. Da waren sie wieder. Der gesamte Bello-Clan führte

weltweite Gespräche (die Nummer 1-49709215 gibt es immer noch), und immer noch scheint Ralph Chukwuma (Tel. 1-234-5891200) der große Pate zu sein. Ziemlich oft konnte das Unwesen eines Dr. Dele Ibrahim (l5451940 und Fax 1-2881474) verfolgt werden. Dummerweise gab er einem „Kunden" in Osterreich seine E-Mail Adresse (deleibrahim@yahoo.co.uk) bekannt, und da mir der Ösi leid tat (er war fast weichgekocht), ließ ich zumindest die E-Mail Adresse sperren. Yahoo reagiert da recht schnell. Unglaublich, aber wahr: genau zu dieser Zeit erreichte einen Mitarbeiter der TSI-Redaktion und mich ein gleichlautendes Angebot eines 65-Millionen Dollar-Deals eines gewissen Dr. Stephen Hozane. Einmal stellte er sich vor als Direktor der National Petroleum Corporation (NNPC) in Lagos, und bei mir als „Top Official from the Federal Ministry of Works and Housing" in Abuja.

Er wurde als mein Opfer ausgewählt. Zum Schein wurde auf den Deal eingegangen. Er bekam den Namen einer Luxemburger Bank und eine Kontonummer genannt; verbunden mit dem zarten Hinweis, das nötige Passwort gebe es erst, wenn er eine Bankgarantie erbringen würde. Hier gab es was für ihn abzuräumen, und er reagierte schneller als die freiwillige Feuerwehr, die manchmal schon vor dem Brand da ist. Per Fax kam die Bankgarantie und eine Telefonnummer (1-888830) mit dem Hinweis, dort am folgenden Tag gegen 21:00 UTC anzurufen. Um es gleich vorweg zu sagen, die Nummer gehört zu keinem Ministerium, sondern ist wahrscheinlich eine gemietete Nummer einer Briefkastenanschrift. Das gesamte Empfangsequipment wurde vorbereitet, und ein kundiger Helfer hatte nicht anderes zu tun, als während des Gesprächs am folgenden Tag Dr. Hazane innerhalb eines drei MHz-Bereiches zu finden. Das heißt, ich musste das Gespräch künstlich verlängern (wer bezahlt mir das eigentlich?)

„Dr.Hazane" schilderte nochmals die Eiligkeit des Deals und reizte mich mit schnell verdientem Geld. Ich erklärte ihm interessiert, dies alles würde ganz gut passen, denn eine Geschäftsreise würde mich folgende Woche eh nach Abuja führen. Da ich auf Einladung einer Organisation dort sei, könnte ich keine Angaben zum Hotel machen, doch die echten Daten des Fluges Frankfurt/Main-Lagos-Abuja bekam er von mir.

Die Gier nach meinem Geld (und ich habe tatsächlich ein Budget für so etwas. Allerdings in Lire, und davon sind

Der Autor ist aufgeflogen - Morddrohung

iiNoiiinoaxa

NATIONAL CORPORATION HEADQUARTERS LAGOS

Bankers

Your Ref: [redacted] Our Ref: JANSO-0597/S2AB [redacted]

PRIVACY

ATTN: [redacted]

We wish to introduce our company/ourselves as a subsidiary of INTERNATIONAL ASSASINATORS AND WORLD SECURITY ORGANZATIONS, with branches in one hundred and two (102) countries.

We have received a fax message our World Headquarters, New York, this morning to inform you to produce a mandatory sum of US$35,000.00 (THIRTY-FIVE THOUSAND UNITED STATES DOLLARS) only, into our account given below in Switzerland within Ninety six hours (96), alternatively, you will kidnapped and forced to commit suicide during the period of our oncoming anniversary of fifty years.

APM AMRO BANK
12 QUAL GENERA GUISAN
1212 Geneva 3
A/C NO. 8270LB (L.N.SIADU)
SWITZERLAND

CAUTION

1. Fax immediately to this office, the payment slip, confirming the payment an to enable us reconcile with our files and deploy our men already monitoring you.

2. We will as well waste no time to carry our operations, if we discover that this contract is disclosed to any second party including the following:-

(a) Police (b) Relation and (C)Friends

3. We guarantee your safety locally and internationally, on the completion of this contract and will not hesitate to disclose our men in your country to you and as well render our service if needed or on request.

We seek your urgent co-operation, for it is not our wish to get you eliminated.

PRINCE (DR) BVANO M. JINOH
SECRETARY

es immerhin 500.000) ließ ihn ein wenig leichtsinnig werden, und so verriet er mir seine Anschrift in Abuja:

Sekou Tour, Crescent/Ecke Ecowas Road (Hausnummern hat man nicht)

Bis hierher wollte ich gehen, denn dies ist in letzter Zeit der kritische Punkt. Wer nämlich abbricht, bekommt eine Mahnung zur Zahlung der angelaufenen Kosten, und die werden dann schon mal mit US$50.000 beziffert. Sollte man nicht zahlen und auch nicht auf den Deal eingehen, gibt es seit etwa in einem Jahr eine Mahnung der besonderen Art, und die kann besonders schädlich für herzkranke oder sensible Menschen sein. Unter dem Absender der „National Assasination and World Security Organization" wird um Begleichung der „Schuld" gebeten, und zwar innerhalb von 96 Stunden. Falls nicht bezahlt wird, sieht man sich zu folgenden Maßnahmen (im Auftrage des Kunden) gezwungen:

, Anderenfalls werden Sie entführt und zum Selbstmord gezwungen. ... Faxen Sie unserem Büro umgehend eine Bestätigung Ihrer Zahlung, oder wir werden den Vorgang abschließen und unsere Männer schicken, die Sie bereits beobachten. Wir werden außerdem nicht zögern, unsere Operation auszuführen, sollten wir herausfinden, dass dieser Vertrag anderen zur Kenntnis gebracht wird; einschließlich Polizei, Verwandte und Freunde."

In der Vergangenheit wurde als Konto die Nummer 8270LB (L.N.SLADU bei der AMRO-Bank in 1212 Genf) angegeben, doch scheint man inzwischen auf eine Offshore-Bank ausgewichen zu sein. Unterschrieben wird der nette Brief durch einen Prince Bvano H. Jimor.

Zumindest hatten wir während des Telefonats das Frequenzsegment für Gespräche Nigeria-Europa ausfindig machen können. In den folgenden Wochen war unser Dr. Stephen Hozane ein recht williges und informatives Opfer. Zwei seiner Klienten konnten frühzeitig gewarnt werden, und auch die „419-Coalition" (eine private Organisation, die seit Jahren die Umtriebe der Scam-Mafia beobachtet und wichtige Details an das FBI und andere Dienste weiterleitet) wurde mit ausreichend Material gefüttert.

So ganz scheint es Nigerias Staatschef Obasanjo nicht ernst zu sein mit seiner Säuberungsaktion im eigenen Haus.

Mehrfach gaben Hozane und andere Mitglieder des Bello-Clans eine Telefonnummer an, unter der sie momentan zu erreichen seien: +234392344107. Sie

gehört zum Informationsministerium des Landes.

Nachtrag

Die in dieser Geschichte beschriebenen Abhörmethoden waren legal, da die Technik in den Niederlanden benutzt wurde und nach geltendem Recht nicht gegen Gesetzt verstoßen wurde.

Diese und andere Stories erscheinen als Serie in der Fachzeitschrift „Tele-Satellit“ und zum Teil später in den Büchern des Autors. Leider sind nicht mehr alle Teile der Serie erhalten, da der Verleger aus dem mageren Online-Archiv alle Spionage-Stories des Autors entfernt hat. Die Berichte erregten teilweise Aufsehen und wurden teilweise in der EU in Brüssel („Das Echelon-System) und im US-Congress („Nigeria Connection“ und „Fax-Interception via Satellite“) diskutiert.

UPDATES

Neuer ‚Live'-Tab für Amazon Fire TV

In der Menüleiste aller Fire TV- und Fire TV Edition-Geräte gibt es jetzt einen neuen Tab: ‚Live'. Über diesen finden Kunden schnell und einfach ihre Live-TV-Apps und -Inhalte. Der ‚Live'-Tab ermöglicht ein bequemes Browsen durch die abonnierten Inhalte und bietet Zugang zur integrierten Senderliste. Zudem lassen sich über den ‚Live'-Tab auch neue Apps finden und herunterladen sowie die Live TV-Einstellungen verwalten.

Im ‚Live'-Tab sind Live-TV-Inhalte und -Apps, lineare Fernsehsender sowie Prime Video Channels zusammengefasst. Die Inhalte sind in Reihen angeordnet. Dazu zählen Kategorien wie ‚Zuletzt verwendete Kanäle' oder ‚Live-Sport', aber auch Reihen für die Sender von voll integrierten Apps. Zum Start sind dies waipu.tv, Red Bull TV und Pluto TV. Auf Fire TV Edition-Fernsehern werden außerdem Reihen für lineare Fernsehsender angezeigt.

Kunden können über den ‚Live'-Tab zudem schnell und einfach auf die Fire TV-Senderliste zugreifen, dort direkt ihre bevorzugten Kanäle auswählen oder sehen, welche Sendungen im linearen Fernsehen, auf Prime Video Channels oder in Apps von anderen integrierten Anbietern laufen.

Der Rollout für den ‚Live'-Tab hat bereits begonnen. Der neue Tab wird in den nächsten Wochen auf allen Fire TV- und Fire TV Edition-Geräten in Deutschland verfügbar sein.

Google: Allianz gegen Android-Malware-Apps

Betrug auf Play-Store-Anwendungen - Zusammenarbeit mit Unternehmer wie ESET

Google schließt mit mehreren Cybersecurity-Firmen ein Bündnis namens „App Defense Alliance“, das gegen Malware-Apps vorgehen soll, bevor sie auf Android-Geräten landen. Zu den Google-Partnern gehören die Unternehmen ESET http://eset.com , Lookout http://lookout.com und Zimperium http://zimperium.com .

Cyber-Kriminellen voraus

„ESET ist seit Langem führend bei der Erforschung neuer Cyber-Bedrohungen. Durch unser Engagement in der App Defense Alliance stellen wir Google weitergehende Informationen bereit, um Android-Bedrohungen schneller zu beseitigen. So werden Android-Nutzer zukünftig Cyber-Kriminellen einen Schritt voraus sein“, meint Tony Anscombe, ESET Global Security Evangelist, gegenüber pressetext.

Um gegen Android-Malware-Apps vorzugehen, integriert Google die Erkennungsfunktionen seiner Cybersecurity-Partner in das eigene „Play Project“-System. Dadurch soll Google wichtige Informationen über Apps von Drittherstellern erhalten, bevor diese im Play Store landen. Play Project arbeitet mit maschinellem Lernen und einer Mischung aus Sicherheitmaßnahmen auf Geräten sowie in einer cloudbasierten Infrastruktur.

Flut an Malware-Apps

Play Project konnte aber bisher nicht die Flut an schädlichen

Apps auf Android stoppen. Erst im September 2019 hat der ESET-Security-Forscher Lukas Stefanko 172 Anwendungen auf Google Play gefunden, auf denen Praktiken wie Werbe- oder Phishing-Betrug vorkamen. Insgesamt hatten diese Apps im September 2019 etwa 335 Mio. Downloads.

Die schädlichen Apps verwendeten unterschiedliche Tricks, um an der Play-Project-Kontrolle vorbeizukommen. Dazu gehören die Anwendung von verschlüsseltem Code oder Command-and-Control-Server, die schädliche Elemente den Apps erst hinzufügten, wenn diese schon auf Google Play erhältlich waren. Mit der App Defense Alliance soll das Kontrollsystem von Google stärker werden und so Android-User vor Malware-Apps bewahren.

DIVEO am Ende!

Die M7-Gruppe stellt die Plattform Diveo zum 30. 11. ein

Die gesetzten Ziele wurden offensichtlich nicht erreicht. Die französische Gruppe M7, die 2017 in Deutschland mit der Plattform Diveo auf den Markt kam, beendet überraschend die Aktivitäten. Diveo, das lineares Satelliten-Fernsehen mit Online-Inhalten verknüpft, wurde vom Endverbraucher nicht so angenommen, wie erhofft. Entsprechende Gerüchte bestätigte Diveo nun gegenüber DWDL.

„Trotz eines innovativen, hervorragenden Endkundenprodukts zu einem sehr günstigen Preis ist es mit dem Sat-Produkt Diveo nicht gelungen, an die Erwartungen und das Wachstum wie im Kabel und bei IPTV anzuknüpfen“, erklärte ein M7-Sprecher. „M7 bedauert diesen Schritt und hat die Endkunden und Partner der Plattform bereits informiert.“

Noch vor rund eineinhalb Jahren gab sich Diveo´s C.E.O. Oliver Rockstein im Quotenmeter.de-Interview hoffnungsvoll: „Mit Diveo platzieren wir ein TV-Produkt am Markt, das konsequent auf die Bedürfnisse und Lebensgewohnten von Konsumenten im digitalen Zeitalter ausgerichtet ist und den sich ändernden Nutzungsgewohnheiten Rechnung trägt. Die Nutzungsdauer der linearen HD-Angebote der öffentlich-rechtlichen und großen privaten TV-Sender bleibt mit rund 221 Minuten pro Tag stabil, gleichzeitig steigt jedoch die Nachfrage nach Video-on-Demand und IP-basierten Diensten. Parallel dazu rufen Konsumenten immer mehr TV-Inhalte über Smartphones und Tablets ab“, erklärte er damals.

Abonnenten dürfen nach dem 30. November ihre Set Top Box behalten. Ein schwacher Trost, denn gerade die Qualität dieses Receivers gab immer wieder Anlass zur Klage bei den Abonnenten.

Streaming

Diese Geräte verlieren am 1.12. den Netflix-Support

Ab dem 1. Dezember 2019 können einige ältere Samsung und Roku Geräte nicht mehr auf Netflix zugreifen. Netflix nennt „technische Einschränkungen“ als Grund für diesen plötzlichen Verlust der Unterstützung, aber es ist unklar, was diese technischen Einschränkungen überhaupt sind.

Der Mangel an Transparenz ist frustrierend, und es kommt noch schlimmer, wenn man versucht herauszufinden welche Geräte nun betroffen sind. Eine vollständige Liste aller betroffenen Geräte ist bisher noch nicht erschienen, aber sowohl Roku als auch Samsung haben einige Hinweise gegeben.

Hier sind zumindest einige der Geräte, die im Dezember nicht mehr unterstützt werden:

Roku-Geräte:
Roku 2000C, Roku 2050X, Roku 2100X, Roku HD, Roku SD, Roku XD, Roku XR

Samsung Fernseher:
Baujahre 2010 und 2011: Fernseher mit einem C oder D im Typenschlüssel. Auf der Support-Seite von Samsung finden Sie den Code Ihres Fernsehers. Beachten Sie, dass der Verlust der Netflix-Unterstützung nur für die Fernseher selbst gilt.

Sie können Netflix weiterhin auf älteren Samsung-Fernsehern ansehen, solange Sie dies über ein Gerät tun, das Netflix derzeit unterstützt.

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/

Online Kiosk

www.onlinekiosk.de

www.tectime.tv

magazin@tectime.tv