TecTime Magazin

Ausgabe 13

NEUES GEWINNSPIEL: VU+ und nixplay

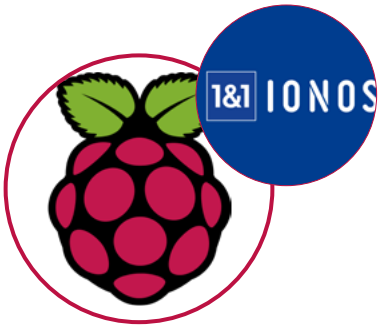
TEST
VU+ Ultimo 4K

TEST
nixplay
Der Smart Foto Rahmen

INVESTIGATIV
Das saudische Königshaus, ARABSAT und die Piratenorganisation beoutQ

Kampf den Stromfressern in der eigenen Wohnung

MEDIEN
Illegale IPTV-Anbieter um die Hälfte dezimiert



Raspberry Pi SERIE
Eigener DNS-Server mit Raspberry Pi

STORY
David gegen Goliath

INHALT

EDITORIAL

Christian Mass

Chefredakteur

Liebe Leser,

vor ein paar Jahren kostete ein Radio-Scanner einige hundert Euro. Heute nimmt man 20 Euro in die Hand und ein Stück kostenloser Software und schon ist man im Besitz ein Breitbandempfängers für den Bereich zwischen 50 und 2.100 MHz.
Na gut, mit den Filtern hapert es, doch die waren bei den Scannern auch nicht besser,

Was bei den Audio-Empfängern funktioniert, sollte doch bei Satelliten-Empfängern möglich sein.
Ja, es gibt erste zarte Versuche. Radioamateure entwickelt SDR-Software für den Empfang von DVB S2 Signalen des Es'Hail-2 Satelliten. Ein anderer arbeitet seit Mai 2019 an einem SDR DVB 2S Receiver. Einfach nur fernsehen kann man natürlich besser auf der Couch vor dem heimischen Flachbildschirm. Doch es gibt immer noch Sat-DXer, die mehr wollen. Satelliten-Signale liefern nicht nur bunte Bilder und Ton, sondern noch Unmengen an technischen und inhaltlichen Zusatzinformationen. Mit einem SDR-Empfänger ließen sich nicht nur Bänder scannen (Blindscan) sondern zu jedem entdeckten Signal würden noch alle relevanten Parameter ablesbar sein. Nehmen wir die Symbolrate, die FEC, Herkunft des Signals und Namen usw. Ein Klick im Spektrum auf das Signal und wir hätten alle wichtigen Informationen zum Sender. Und von dort ist es dann auch nicht mehr weit zur spannenden Satelliten-Spionage wie Ende des vergangenen analogen Jahrhunderts.
Die meisten digitalen Formate (Daten und Telefonie) sind heute kein Geheimnis mehr.
Es müssen nur die Macher her.
Und sie werden kommen!

Herzlichst,

Euer Dr.Dish

Impressum
Herausgeber, Chefredakteur und verantwortlich für den Inhalt
Christian Mass | mass@tectime.tv | Naupliaalle. 22, 85521 Ottobrunn

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

Äthiopien startet im Dezember den ersten Satelliten

Der äthiopische Präsident Sahle-Work Zewde teilte vor einer Woche mit, dass Äthiopiens erster Satellit im Dezember dieses Jahres mit Unterstützung der chinesischen Regierung ins All gestartet wird.

„Der erste äthiopische Satellit wird im Dezember dieses Jahres von einem Zentrum in China aus gestartet“, sagte Zewde vor der neuen Parlamentssitzung des Äthiopischen Hauses der Volksvertreter (HoPR) und des Hauses der Föderation (HoF), die kürzlich in einer gemeinsamen Sitzung eröffnet wurde.

Äthiopien entwickelt derzeit mit Unterstützung der chinesischen Regierung den ersten Satelliten des Landes, einen 70 kg Multispektralen Fernerkundungssatelliten, bekannt als ETRSS-1.

Laut Zewde sieht die äthiopische Regierung vor, dass der erste Satellit des Landes, sobald er seinen Betrieb aufnimmt, die Bemühungen des ostafrikanischen Landes zur Modernisierung seines Agrarsektors unterstützen wird.

„Der Satellit wird alle notwendigen Daten über Veränderungen des Klimas und wetterbedingter Phänomene liefern, die für die wichtigsten Ziele des Landes in der Land- und Forstwirtschaft sowie für Initiativen zum Schutz natürlicher Ressourcen genutzt werden“, sagte Zewde vor den Mitgliedern der beiden Häuser.

Der Satellit, der von China aus gestartet werden soll, wird sein Kommando- und das Kontrollzentrum in Äthiopien in der Weltraumüberwachungs-Station Entoto haben - Ostafrikas einzige Station auf den 3.200 Meter hohen Bergen von Entoto am Rande der Hauptstadt Addis Abeba.

Im April dieses Jahres hatte der äthiopische Premierminister Abiy Ahmed auch die China Academy of Space Technology besucht, um den 70 kg schweren multispektralen Fernerkundungssatelliten ETRSS-1 zu inspizieren.

ETRSS-1 wird u.a. das Wetterverhalten für eine bessere landwirtschaftliche Planung, Dürrefrühwarnung und Forstwirtschaft überwachen.

Quelle: Xinhua

VU+ Ultimo 4K

Im Kurzstest

Seit Vu+ den Ultimo4K auf der Anga Cable 2016 vorstellte ist einige Zeit vergangen. Im Laufe der Jahre wurde einige Bugs getilgt und der Ultimo 4K erfreut sich allgemeiner Beliebtheit.

Sehen wir uns das aktuelle Modell etwas genauer an:

Der Ultimo4K hat ein schönes großes 4,0“ TFT-Display auf der Vorderseite, dies ist eine schöne Größe, da es viel Platz hat, um Kanalnamen, Programmnamen, Start-/Endzeiten, Fortschrittsbalken und auch die aktuelle Zeit anzuzeigen. Es kann auch konfiguriert werden, um ein Kanal-Picon anzuzeigen, und aufgrund seiner Größe ist dies wiederum sinnvoll.

Alternativ können Sie das 4,0“-Display als MiniTv verwenden und es zeigt das aktuelle Programm auf dem Display an, dies ist nützlich, wenn Sie den Fernseher nicht einschalten möchten. Sie können den Fernsehkanal weiterhin mit einem Paar Bluetooth-Kopfhörer oder einer Soundbar hören.

Das Innenleben

Im Inneren des Ultimo4K befinden sich hinten rechts die steckbaren FBC-Tuner. Der Ultimo4K wird mit austauschbaren Tunern geliefert, FBC steht für Full Band Capture. Hier wäre z.B. eine gute Kombination 1x DVB-S2X FBC Twin / 1x DVB-C FBC / 1x DVB-S2 Dual Tuner PVR ready.

Der DVB-S2 FBC Twin Tuner besitzt 8 Demodulatoren. Bei zwei herkömmlichen (z.B. Twin-LNB) Sat-Zuleitungen ist der Tuner mit 2 herkömmlichen und 6 zusätzlichen Tunern, die im Durchschleifbetrieb arbeiten, vergleichbar. Man kann somit Sender aus 8 verschiedenen Transpondern aus 2 unter-

schiedlichen Sat-Ebenen gleichzeitig ansehen, streamen oder aufnehmen. Im SCR-Betrieb (Unicable) mit 8 Frequenzen entspricht dies 8 herkömmlichen Tunern.

Der DVB-C FBC Tuner besitzt 8 Demodulatoren. Dies entspricht einem Receiver mit 8 herkömmlichen DVB-C Tunern.

Somit kann man 8 Sender zur gleichen Zeit ansehen, streamen oder aufnehmen.

Der große schwarze Kühlkörper, der in der Mitte sichtbar ist, deckt den Broadcom BCM 7444s 1,5 GHz Quad Core 20.000 DMIPS ARM v7 CPU ab. Vorne rechts gibt es die Kartenleser und CI-Slots. Die Halterung für die interne Festplatte befindet sich vorne links, und man kann entweder eine 2,5“ oder 3,5“ Festplatte im Ultimo4K montieren. Ein Netzteil sucht man im Inneren vergebens, denn die Stromversorgung erfolgt extern und das hält die Temperatur im Inneren niedrig.

Bluetooth 4.0

Der Ultimo4K verfügt über Bluetooth 4.0, dies kann verwendet werden, um eine Verbindung zu einer Soundbar oder zu einem Paar Bluetooth-Kopfhörer herzustellen, was nützlich ist, wenn man das Frontdisplay als MiniTv verwendet. Das Bluetooth wird jedoch nicht mit einem iPhone oder einem ähnlichen Gerät verbunden.

Wi-Fi

Der Ultimo4K hat ein Wireless Lan eingebaut und unterstützt sowohl 2,4 GHz als auch 5 GHz Bänder.

HDMI-Eingang

Eine schöne Funktion, die Vu+ hier hinzugefügt hat. Dies gibt dem Nutzer die Möglichkeit, ein anderes Media-Gerät an den Ultimo 4K anzuschließen, und es bedeutet, dass man nur die eine HDMI-Verbindung zum Fernseher benötigt. Dies funktioniert möglicherweise nicht mit allen Geräten, da der Kopierschutz HDCP 2.2 nicht gewährleistet ist.

HbbTV

Der Ultimo4K unterstützt auch HbbTV. Einfach einen Sender einstellen, der den Service bietet und dann den roten Knopf der Fernbedienung drücken. Der Ultimo 4K wird dann die Internetverbindung nutzen, um sich mit den On-Demand-Diensten des Senders zu verbinden.

IPTV

Der Ultimo 4K bietet die Möglichkeit IPTV entweder über Plugins oder direkt aus der Kanalliste (Bouquets) zu nutzen, wenn man IPTV aus den Bouquets wählt.

Blindscan

Ein weiteres tolles Feature des Ultimo 4K ist die Blindscan-Funktion, dies ist eher für Enthusiasten und fortgeschrittene Benutzer gedacht, die den Clark Belt nach allen Kanälen durchsuchen möchten, die sie finden können. Das Blindscan-Plugin fordert auf, den Satelliten auszuwählen, den man absuchen möchte und dann erledigt der Empfänger den Rest. Es ist eine großartige Funktion, besonders bei der Suche nach Feeds.

In der Praxis

Im Kurztest wurde der Ultimo 4K an eine drehbare Antenne angeschlossen. Die Internet-Anbindung lässt Ethernet als auch WLan zu. Wie bereits erwähnt, gibt es im Ultimo 4K Platz für eine interne Festplatte (2,5“ oder 3,5“), aber man kann auch eine Netzwerk-HDD verwenden, wenn ein NAS-Setupvorhanden ist.

Der Ultimo 4K schafft den Kaltstart in etwa 33 Sekunden. Diese Zeit variiert je nachdem wie viele Plugins, Skins usw. installiert sind. Übrigens, der Neustart aus dem Standby-Modus dauert nur 13 Sekunden Der erste Suchlauf auf HOTBIRD war in ca. 8 Minuten erledigt. Alternativ dazu lassen sich auch Kanallisten von Anbietern im Internet oder vom Addons Server verwenden.

Ultra HD

Der Ultimo 4K gibt Fernsehbilder in vie-

len verschiedenen Auflösungen aus, so dass man keinen Ultra HD Fernseher benötigt, um diesen Receiver zu verwenden, denn das Betrachten von 4K UHD-Inhalten auf einem 1080p Fernseher wirft die Frage auf, ob man überhaupt einen 4K Fernseher benötigt, da das Bild hell und klar ist. Wie wichtig ein 4K Fernseher ist, sieht am erst wenn echte UHD-Inhalte gesendet werden. Die Brillanz und die Tiefen sind unübertroffen. Leider hält sich die Anzahl der UHD-Sender in Grenzen.

Fazit

Der Ultimo 4K hat dank seines Quad Core Prozessors (mehr als seine kleine Schwester Solo4K oder der kleine Bruder Uno4K, die beide Dual Core sind) viel Rechenleistung, das bedeutet schnelle Boot-Up- und Restartzeiten, schnelles Kanal-Zappen und vor allem Stabilität. Der Ultimo 4K ist kein billiger Empfänger und wird mit Sicherheit die Satelliten-Freaks ansprechen, da er über Funktionen verfügt die der Enthusiast benötigt.

Sollten Sie man den Ultimo4K kaufen? Vom Autor gibt es hier nur ein klares JA als Antwort. Allein schon die Flexibilität bei der Tuner-Auswahl sind schon das Geld der Anschaffung wert. Aber auch im „normalen“ Wohnzimmer tut der Ultimo 4K seinen Dienst als komfortabler und hochwertiger Familien-Receiver.

Technische Daten:

- 1.500 MHz ARM QuadCore-Prozessor (20.000 DMIPS)
- 4096 MB Flash (eMMC)
- 3072 MB DDR3 DRAM
- Gigabit LAN (10/100/1000 MBit/s)
- Wlan: IEEE 802.11 b/g/n/ac 2,4 / 5 GHz integriert
- Wake on Wireless LAN (WoWL)
- BT 4.0 integriert für z.B. BT Soundbars oder Kopfhörer
- 2x DVB Common-Interface Einschub
- 2x Smartcard-Reader (Xcrypt)
- 2x USB 3.0 (Rückseite)
- 1x USB 2.0 (Vorderseite)
- 4,0“ TFT LCD Display - MiniTV
- S/PDIF Audio Ausgang optisch (digital)
- 2 x Audio Ausgang (L/R) RCA (analog)
- 1x HDMI 2.0 Video/Audio Ausgang (digital)
- 1x HDMI 2.0 Video/Audio Eingang (digital)
- unbegrenzte Kanalliste für TV und Radio
- EPG (Electronic Program Guide) Unterstützung
- Unterstützung von Bouquet-Listen (Favoritenlisten)
- OSD in vielen Sprachen
- Aussehen der Benutzeroberfläche vielfältig anpassbar (Skin-Unterstützung)

- Erweiterbar durch viele kostenfreie Plugins (Apps)
- automatischer / manueller Kanalsuchlauf
- DiSEqC 1.0/1.1/1.2, USALS
- SCR / CSS (EN50494 & EN50607)
- Externes 12 Volt Netzteil
- Netzschalter
- RS232 - Serviceschnittstelle
- kostenfreie Apps für iOS und Android verfügbar

Videodekodierung:

- Videokompression HVEC / H.265, MPEG-2 / H.264 und MPEG-1 kompatibel
- Videostandard PAL G/ 25 Hz, NTSC
- Bildformat 4:3 / 16:9
- Letterbox für 4:3 TV-Geräte

Ausgang Digital:

- Abtastfrequenzen 32 kHz, 44.1 kHz, 48 kHz
- S/PDIF-Ausgang optisch (AC3)
- Audiokompression MPEG-1 & MPEG-2 Layer I und II, MP3
- Audio Mode Dual (main/sub), Stereo
- Abtastfrequenzen 32 kHz, 44.1 kHz, 48 kHz, 16 kHz, 22.05 kHz, 24 kHz

Leistungsaufnahme:

< 26W (im Betrieb, mit LNB)

< 25W (im Betrieb, ohne LNB)

< 0,5W (Deep-Standby-Mode)

Externes Netzteil:

- Eingang:
  110 - 240V AC / 50 - 60Hz / 1,5A
- Ausgang: 12V = / 5,0A

Allgemeines:

- Umgebungstemperatur +15°C...+35°C
- Luftfeuchtigkeit < 80%
- Abmessungen (B x T x H): 380 mm x 290 mm x 78 mm
- Gewicht: 2,9 kg

Lieferumfang:

1x VU+ Ultimo 4K UHD Receiver

1x Fernbedienung

1x Quickmanual
(deutsch / englisch)

1x HDMI Kabel

2x Batterien (AAA)

1x Netzteil (110-240V / 12V)

* DVB-C FBC Tuner werden nur in Tunersteckplatz A unterstützt

TECHNIK

Elektronischer Bilderrahmen Nixplay Smart Photo Frame W10E

Haben Sie schon einmal darüber nachgedacht, was man mit den unzähligen eigenen Fotos machen soll, die seit ewigen Zeiten das Memory ihres Handis füllen? Eine elegante Lösung biet das Unternehmen Nixplay mit dem Smart Photo Frame W10E an. Die „10“ im Namen steht für die Bildschirmdiagonale von 10 Inches. Genauer gesagt es sind eigentlich 9,7 Inches und das wären dann 24,638 Zentimeter. So kommen die besten eigenen Fotos endlich zu Ehren, da sie als Dia-Show auf dem Nixplay Fotorahmen erscheinen.

Einmal ausgepackt finden wir neben dem eigentlichen Rahmen eine kleine Fernbedienung, einen Steckeradapter, das Netzteil, Montagematerial für die Befestigung an einer Wand und natürlich die Betriebsanleitung. Diese war beim Testmodell leider nur in englischer Sprache vorhanden. Nicht allzu schlimm für den Eigner des Smart Phone Frame, da die Funktionen sich eigentlich von selbst erklären.

Der Foto-Rahmen hat auf der Rückseite einen flexiblen Ständer, sodass die Schräge des Bildschirms den eigenen Bedürfnissen leicht angepasst werden kann. Der Bildschirm kann horizontal oder vertikal aufgestellt werden. Wird der Nixplay an der Wand montiert, dann wird der Ständer auf der Gleitschiene rausgeschoben und an seiner Stelle findet die Montageplatte ihren Platz.

Zwei Sensoren auf der linken Seite des Rahmens reagieren auf Bewegung oder auf die mitgelieferte Fernbedienung. Parktisch ist der Bewegungs-Sensor, da dann der Bildschirm mit Fotos nur aktiv wird, wenn er eine Bewegung feststellt. Zum Beispiel wenn jemand den Raum betritt. Bewegt sich nichts, schaltet der Bildschirm nach einer voreingestellten Zeit ab und wird dunkel. Oder ab er stellt eine Uhr dar.

Über die Fernbedienung wird das Gerät ein – oder ausgeschaltet. Die Wiedergabelisten können aktiviert werden und die Art des Übergangs zwischen den einzelnen Fotos. Über + und – Tasten wird die Lautstärke geregelt. Die Tasten sind logisch angeordnet und mit leicht einprägsamen Symbolen versehen.

In der Praxis

Erst einmal sollte am sich die Nixplay App (Android oder I.O.S.) besorgen. Die ist kostenlos. Über die URL www.nixplay.com erfolgt die Registrierung. Die Verbindung der App mit dem Nixplay ist kinderleicht. Ist dann ein Konto erstellt, kann es losgehen. Über die App lassen sich Fotos und Videos hinzufügen, Ja Videos laufen auch, doch leider nur maximal 15 Sekunden. Hier sollte der Hersteller nachbessern. Die App speichert die Inhalte auf dem Nixplay-server. 19 GB sind kostenlos. Das sollte eigentlich für den normalen Betrieb langen.

Sind die Fotos und Videos für eine Playliste gefunden, dann sendet das Mobiltelefon diese Inhalte den an den Nixplay.

Bei der Einstellung der Bild-Übergänge und der Darstellung gibt es kaum Grenzen. Es kann geschwenkt, gezoomt oder gedehnt (keine schwarzen Ränder) werden.

Ganz Mutige geben Freunden oder Kanälen aus den sozialen Netzwerken den Zugang zum Bildschirm.

Fazit

Der Nixplay Smart Photo Frame W10E unterscheidet sich durch sine vielen Funktionen deutlich von elektronischen Bildschirmen der Wettbewerber. Die Bildschirmauflösung von 2048×1536 ist mehr als nur gut. Auch bei der Verarbeitungsqualität gibt es nichts auszusetzen. Einziges Manko ist die unzureichende Laufdauer der Videos mit maximal 15 Sekunden. Mit rund 280,- Euro zählt der Bildschirm nicht gerade zu den Schnäppchen, doch dafür bietet er auch eine ganze Menge.

Technische Daten

- **Geräteabmessungen:**
  19.9 x 24.8 x 3 cm
- **Nettogewicht:**
  572g
- **Bildschirmauflösung:**
  2048×1536; 2K
- **Seitenverhältnis:**
  4:3
- **Bildschirmhelligkeit:**
  350 cd/m2
- **Unterstützte Foto-Format:**
  JPEG / JPG
- **Speicher / RAM:**
  8GB / 1GB
- **Sensoren:**
  Hu Motion
- **Lautsprecher:**
  2 x (2W)
- **W-Lan:**
  802.11 b/g/n

Anbieter: www.nixplay.com

TECHNIK

Kampf den Stromfressern in der eigenen Wohnung

Immer mehr Deutsche sind online! Die Zahl der Internetnutzer steigt und steigt. Und auch die Internetnutzungsdauer wächst kontinuierlich.

Natürlich liegt das auch daran, dass schnelles Internet immer mehr Verbreitung findet und zunehmend auch ländlichere Gebiete erschlossen werden. Der DSL-Router fällt in den meisten Haushalten schon gar nicht mehr auf, sondern ist schon fest integriert. Dass dem Gerät meist keine große Beachtung geschenkt wird, heißt aber genauso, dass es läuft und läuft und läuft – und entsprechend viel Strom frisst.

Jeder fünfte Deutsche ist ein sog. Abschaltmuffel – wenn es darum geht, die Energiekosten im eigenen Haushalt zu reduzieren. Das hat eine Studie von TNS-Infratest jetzt ans Licht gebracht.

So lässt beinahe jeder fünfte Befragte sein Fernsehgerät auch bei längerer Abwesenheit im Standby-Modus anstatt es komplett vom Netz zu trennen. Computer, Monitore, DVD-Player oder Drucker werden auch vielfach einfach der Bequemlichkeit willen nicht vollständig ausgeschaltet, sondern verbleiben im Bereitschaftsmodus. Oftmals dauert der vollständige Neustart ein paar Sekunden länger oder ein weiterer Druck auf die Fernbedienung ist notwendig – je mehr Aufwand, desto praktischer und angenehmer erscheint der Standby-Betrieb

Hinzu kommt, dass viele Geräte meist nur die Wahl bieten zwischen Standby und Stecker ziehen. Der Netzschalter wie ihn beispielsweise zahlreiche Sat-Receiver mittlerweile fest eingebaut haben, wäre noch eine gute Alternative. Sie brauchen nicht extra den Stecker zu ziehen, das Gerät ist aber dennoch ausgeschaltet. Manche Produkte ziehen aber sogar in diesem Zustand noch eine geringe Menge Strom.

Obwohl die Verschwendung insgesamt wohl relativ verbreitet ist, gibt beinahe jeder Befragte an, er versuche, die Kosten nach Möglichkeit zu reduzieren und Standby-Betrieb zu vermeiden. Anscheinend siegt dann aber doch oftmals wieder die Bequemlichkeit oder die Gewohnheit, ähnlich wie bei guten Vorsätzen für das neue Jahr.

Wenn es in den verdienten Urlaub geht, bleibt das Telefon mitsamt Anrufbeantworter bei vielen an – und das obwohl die meisten sowieso ihr Handy mit auf Reisen nehmen. Internet- und DSL-Router genauso. Sogar beinahe 40 Prozent der Befragten lassen ihr Faxgerät an wenn sie längere Zeit weg sind.

Insgesamt ergibt sich laut TNS Infratest eine Summe von knapp 100 Euro pro Jahr – Stromkosten durch überflüssigen Standby-Betrieb. Dieses Geld wäre anders sicher sinnvoller investiert. Um

ganz sicher zu sein, können Sie sich auch ein Strom-Messgerät bei der Verbraucherzentrale oder einem Stromerzeuger ausleihen und direkt nachmessen, ob Ihre Geräte auch nach dem Ausschalten noch Strom verbrauchen. Das Messgerät wird zwischen Netzstecker und Steckdose geschaltet. Sie sehen dann die Leistungsaufnahme in Watt.

Wie können Sie sonst am einfachsten die eigene Bequemlichkeit überlisten?

Wenn schon an den Geräten kein ON-OFF-Netzschalter vorhanden oder dieser nur schwer erreichbar ist – dann macht auf jeden Fall eine Stecker-Leiste Sinn, die Sie ein- und ausschalten können.

Natürlich sollte diese dann günstig zu erreichen sein und sich beispielsweise nicht gerade hinter einer Schrankwand befinden.

Alternativ wäre auch der Einsatz von Funk-Steckdosen eine gute Möglichkeit, gleich mehrere Geräte auf einen Schlag auszuschalten. Die Steckdosen mit Fernbedienung sind günstig im Elektrofachhandel zu bekommen. o hätten Sie es immer noch sehr bequem und praktisch – und müssen nicht zu viele umständliche Handgriffe in Kauf nehmen. Schließlich können Sie auch ein sog. Vorschaltgerät einsetzen, um unnötigen Stromverbrauch durch Standby-Betrieb zu vermeiden.

Einmal vorgeschaltet wird das angeschlossene Gerät nach einer bestimmten Zeit automatisch vom Netz getrennt.

Was können Sie nun machen, um Standby-Betrieb zunächst zu erkennen?

Überprüfen Sie, ob das Gerät auch längere Zeit nach dem Ausschalten noch warm ist. Dies ist ein sicheres Anzeichen dafür, dass weiterhin Strom fließt.

Auch ein Brummen oder Surren nach dem Ausschalten ist sehr verdächtig und zeigt Ihnen, dass immer noch Kosten entstehen.

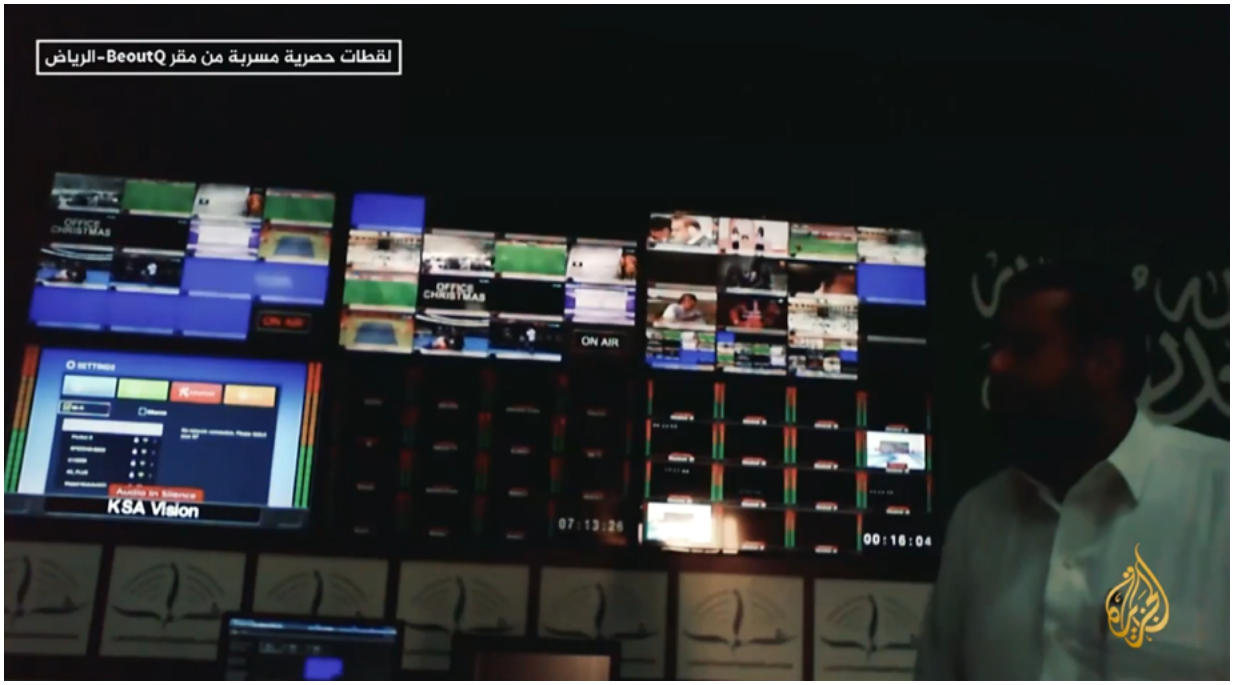
Demnächst NEU bei TecTime:

TecT.....

INVESTIGATIV

beoutQ die Zweite

beoutQ Piraten-Standort ermittelt



In der Ausgabe 5 des TecTime-Magazins wurde erstmals über die Machenschaften der saudischen Piratensendergruppe beoutQ berichtet und wir konnten einen Beteiligten – den C.E.O. Dr Raed Khusheim der Firma Selevision – ermitteln. Doch er ist nicht der einzige Beteiligte. Hinter beoutQ steckt die ARABSAT-Organisation und das saudische Könighaus. Hier ein Blick zurück:

Wie aus beIN Sports plötzlich beoutQ wurde

beIN Sports ist ein Sportkanal, der im November 2003 ursprünglich als Al Jazeera Sport gegründet wurde. Heute verfügt der Sender über 19 HD-Kanäle und gehört der beIN Media Group - ein Tochterunternehmen von Al Jazeera - an, die ihren Sitz in Doha hat. Seit 2014 wird das PayTV-Paket beIN Sports über die Badr Satelliten abgestrahlt und hat einige Millionen Abonnenten.

Die meisten in Saudi-Arabien und in den Vereinigten Arabischen Emiraten. beIN Sports besitzt u.a. die Rechte an der Bundesliga, der Fußball EM und WM und der Formel 1 in der Region.

Nach dem 5. Juni 2017 (dem Tag an dem Saudi Arabien die Beziehungen zu Katar abbrach) tauchten auf den Badr-Satelliten plötzlich 10 Sender unter der Bezeichnung beoutQ auf. Gleichzeit warb beoutQ in der Region aggressiv für die speziellen Set-Top-Boxen für den Empfang von beoutQ via Satellit und IPTV. Für rund 95 Euro.

Die Nachfrage nach den Boxen und Abonnements war immens. Und wer nun Zugang hatte, der empfing mit einer Zeitverzögerung von ca. 10 Minuten die originalen Inhalte vom Rechtehalter beIN Sports. Das beIN-Logo verschwand hinter einem Overlay des beoutQ-Logos. In derselben Zeit wurden die Übertragungen von bein Sports durch ARABSAT geblockt.

Der Weltfußball-Verband FIFA und der Rechteinhaber beIN Media legten sofort Beschwerde bei der ARABSAT Organisation in Ryad, Saudi-Arabien ein, doch deren Antwort war mehr als verwunderlich: “Arabsat war sich von Anfang an sicher, dass das Satellitennetz von beoutQ nicht genutzt wurde”, sagte der C.E.O. Khalid Balkheyour in der Arabsat-Erklärung. „Dennoch haben wir eine sehr kostspielige Untersuchung durchgeführt, um alle Zweifel auszuräumen und Beweise zu liefern, die wir mit der FIFA und der Welt teilen können. Arabsat wurde durch die Angriffe von beIN und der FIFA zutiefst beleidigt und geschädigt”, erklärte er. “Nun, da sich die FIFA-Vorwürfe als falsch erwiesen haben, sollte sie sich für solche beleidigenden Äußerungen entschuldigen.”

Seitdem haben zwar immer wieder internationale Sportorganisationen und Rechteinhaber gegen beoutQ geklagt und auch gewonnen, doch eine zustellbare Adresse des Senders gab es nicht. Saudi-Arabien verweigerte jegliche Unterstützung und lies Gerüchte verstreuen, die Sendergruppe habe ihren Sitz in Nordafrika.

Al Jazeera liefert Beweise

Dann kam der 22. September 2019. Am Abend dieses Tages strahlte das investigative Programm „What lies below“ von Al Jazeera eine Dokumentation zum Thema beoutQ aus, die zeigte, wie zwei saudische Dienstleister, Selevision und Shammas, an den von beoutQ durchgeführten Operationen beteiligt waren. Selevision ist im Besitz der Khusheim

Dr.Raed Khusheim.

Holding und der C.E.O. ist Dr.Raed Khusheim. In den USA registrierte er die Domain „beouQ“ und bezahlte mit seiner persönlichen Kreditkarte, wie das TecTime Magazin ermittelte.
Dr. Khusheim (Vorgespräch mit dem Autor zu einem Interview in Dubai 2007) steht nach eigenen Angaben dem saudischen Königshaus sehr nahe.

In der Dokumentation bewies „What lies below“ erstmalig, dass beoutQ seinen Sitz am Hauptsitz von Selevision im al-Qirawan-Distrikt der saudischen Hauptstadt Riad hat. Das Video zeigt die Uplink-Anlage und Büros und als Beweis das Foto eines Selevision-Dienstwagens vor der Anlage. Das Filmmaterial enthielt auch Bilder des Hauptkontrollraums und der Server, die die gestohlenen Inhalte von bein Sports übernehmen, das Logo ersetzen und als beoutQ abstrahlen. Das Programm Al Jazeera konnte Dokumente vorweisen, die belegen, dass finanzielle Transaktionen zwischen dem saudischen Unternehmen und dem Management von Arabsat stattgefunden haben.

Die Dokumente enthüllten auch, dass ein alternativer Standort für die Piraterieoperationen in einem unbenannten nordafrikanischen Land diskutiert wurde, nachdem Saudi-Arabien unter zunehmendem Druck stand, die Ausstrahlung des raubkopierten beIN-Signals einzustellen.

Saudi-Arabien hat zuvor Behauptungen zurückgewiesen, dass beoutQ seinen Sitz im Königreich hat.

Die Staatsanwaltschaft Katars hat drei Mitarbeiter der beIN Media Group beschuldigt, mit Saudi-Arabien und Ägypten zu kommunizieren, um den Interessen des Sportnetzwerks zu schaden.

In einem Interview mit Al Jazeera sagte die katarische Staatsanwaltschaft, dass einer der drei Angeklagten nach der Durchsetzung der Blockade nach Saudi-Arabien gereist sei.

Der Angeklagte, der ohne Visastempel in seinem Reisepass in das Königreich einreiste, traf den saudischen Geheimdienstmitarbeiter Maher Mutreb und gab geheime und sensible Informationen an den ägyptischen Geheimdienst weiter.

Mutreb ist ein saudischer Geheimdienstler, der für einen Senior Adviser des saudischen Kronprinzen Mohammed bin Salman (MBS) arbeitete. Laut einem Bericht des Sonderberichterstatters der Vereinten Nationen über außergerichtliche Hinrichtungen war

Mutreb eng an der Ermordung des saudischen Journalisten Jamal Khashoggi am 2. Oktober im Konsulat des Landes in Istanbul beteiligt.

Die investigative Arbeit von Al Jazeera ergab, dass die Piraterie-Operation nicht das Ergebnis gewöhnlicher Hacker war, wie Saudi-Arabien seit langem behauptet, sondern Teil eines integrierten Systems mit offizieller saudischer Abdeckung und finanzieller Unterstützung war.

Nachtrag

Auch in Europa bewegt sich was. Ein erstes Urteil gegen einen illegalen Vertrieb von beoutQ-Boxen und Inhalten wurde gefällt. Auch in Deutschlang gibt es beoutQ Angebote für eine Kundschaft in Berlin und in NRW. Passiert ist bisher nichts.

Ein Einzelhändler in London wurde in London wegen der Verletzung des Urheberrechts, Betrugs und dem Vertrieb von illegalen Streaming-Geräten verurteilt. Der Händler vertrieb beoutQ-Streaming-Boxen im großen Stil. Die Klage war das Ergebnis investigativer Zusammenarbeit zwischen der Premier League, der Federation Against Copyright Theft (FACT) und der Polizei.

Auch in Deutschlang gibt es beoutQ Angebote für eine Kundschaft in Berlin und in NRW. Passiert ist bisher nichts

STORY

David gegen Goliath
Herr Frank B. und die Bundesnetzagentur

Um es gleich vorweg zu sagen: es geht in dieser Geschichte um einen durch die Bundesnetzagentur initiierten Polizeieinsatz bei einem Schwerbehinderten und die Beschlagnahme eines GPS-Trackers.


PAJ
GPS
GPS EASY FINDER
SOS
PAJ
FIND & PROTECT

Der Markt für GPS-Sender wächst. So kommt es, dass Behörden, wie die Bundesnetzagentur (kurz: BNetzA) auf die kleinen Peilsender aufmerksam werden. Zu den Aufgaben der BNetzA zählen die Aufrechterhaltung und Förderung des Wettbewerbs in sogenannten Netzmärkten. So auch der Elektrizitäts- und Telekommunikationsmarkt. Unter anderem überprüft die Bundesbehörde Geräte am Markt auf ihre Tauglichkeit gegenüber dem Gesetz.

Das berühmteste Beispiel ist hierbei die erste internetfähige Spielzeugpuppe. Die Puppe „My Friend Cayla" verfügte über ein bluetoothfähiges Mikrofon. Dieses ungesicherte Extra, welches Unbefugten erlaubte Unwissende abzuhören, führte letztendlich dazu, dass das Spielzeug vom Markt genommen werden musste. Familien im Besitz der Puppe wurden zur Vernichtung aufgefordert.

Wie wurde aus einem legalen GPS-Tracker ein illegaler?

GPS-Tracker sind im Allgemeinen absolut legal. Bei der Frage legal oder nicht, spielt lediglich die Fähigkeit private Gespräche abzuhören eine Rolle.

Ähnlich wie „Cayla" besitzen nämlich viele GPS-Sender eine Mikrofon-Funktion. An sich ist das natürlich kein Verbrechen. Jedoch betritt man an dieser Stelle nach §90 des Telekommunikationsgesetzes (TKG) eine rechtliche Grauzone.

„Es ist verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören"

Probleme macht hier die Formulierung Gegenstände des alltäglichen Gebrauchs. Ist ein GPS Tracker ein Alltagsgegenstand? Die wachsende Anzahl an GPS-Geräten gab den entscheidenden Impuls für die BNetzA, diese Frage mit JA zu beantworten. Infolgedessen wurden GPS-/GSM-Sender im März 2018 in die Liste der Gegenstände des alltäglichen Gebrauchs aufgenommen.

Welche Folgen hat das neue Gesetz?

Durch diese kleine Änderung im Gesetz kam es dazu, dass GPS-Tracker mit Mikrofon-Funktion plötzlich nicht mehr legal waren. Demnach verstoßen sowohl Hersteller, Vertreiber als auch die Besitzer eines solchen Gerätes gegen das Gesetz.

Und hier kommt nun unser Leser Frank B. ins Spiel. Da er stark behindert ist, wollte er sich für den Notfall wappnen. Er kaufte sich lange vor der Änderung des § 90m des TKG über Amazon.de den GPS-Tracker EASY Finder 2.0 bei der renommierten Firma PAJ. Dieser Tracker erfüllte die Anforderungen des

- 5 -

bb) Erforderlichkeit

Erforderlich ist eine Maßnahme dann, wenn kein gleich wirksames, aber weniger belastendes Mittel zur Zweckerreichung gegeben ist.

Ein gleich geeignetes, weniger einschneidendes Mittel als die rechtskonforme Umrüstung oder Vernichtung ist nicht ersichtlich. Durch die Möglichkeit der rechtskonformen Umrüstung behält der GPS-Tracker seine Grundfunktionalität des Ortens von Personen oder Gegenständen.

Die Anordnung der Rücksendung an den Verkäufer oder die Verpflichtung des Verkäufers zum Rückruf des rechtswidrigen Mikrofons ist kein gleich geeignetes Mittel, da es dann lediglich zu einer Verlagerung des rechtswidrigen und strafbewehrten Besitzes hin zum Verkäufer käme. Das Ziel, das strafbewehrte Verbot des Besitzes von getarnten, sendefähigen Mikrofonen, durchzusetzen und damit Angriffe auf die Privatsphäre Dritter, die durch den Einsatz dieses Mikrofons ermöglicht werden, wirksam zu unterbinden, könnte durch eine derartige Anordnung damit nicht erreicht werden.

cc) Angemessenheit

Angemessenheit bedeutet, dass die Maßnahme nicht zu einem Nachteil führen darf, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht. Unverhältnismäßig ist eine Maßnahme nur dann, wenn sie zu Nachteilen führt, die erkennbar außer Verhältnis zu dem erstrebten Erfolg stehen, d.h. wenn der durch die Maßnahme herbeigeführte Nachteil deutlich größer ist als der Nachteil, der durch sie abgewendet werden soll. Dies ist vorliegend zu verneinen.

Der Schutz der Privatsphäre ist ein aus Art. 1 Abs.1 und Art. 2 Abs. 1 Grundgesetz abgeleitetes hohes Gut unserer Verfassung. Von einem getarnten sendefähigen Mikrofon, wie es hier in Rede steht, geht aufgrund ihrer Beschaffenheit eine erhebliche Gefahr aus, dass mit ihr unbemerkt Audioaufnahmen von arglosen Dritten aufgenommen werden. Durch die Vernichtungsanordnung mit der gleichzeitigen Nachweisverpflichtung soll diese Gefahr, die von diesem Mikrofon ausgeht, endgültig beseitigt werden.

Der durch die Umrüstungs- bzw. Vernichtungsanordnung für Sie entstehende Nachteil besteht darin, dass die von Ihnen für das Mikrofon getätigte Investition durch die Vernichtung des Mikrofons mangels Rückerstattung des Kaufpreises durch den Verkäufer möglicherweise verloren geht. Diese Investition ist jedoch nicht von der Rechtsordnung geschützt, da der ihr zugrunde liegende Kaufvertrag gegen ein gesetzliches Verbot verstößt. Daher ist die von Ihnen getätigte Investition nicht als ein ins Gewicht fallender Nachteil zu werten.

Weiter sind Sie durch die Anordnung der Nachweiserbringung über die rechtskonforme Umrüstung oder Vernichtung belastet. Die Nachweiserbringung ist ein kaum ins Gewicht fallender Nachteil, da er weder stark zeit- noch kostenintensiv ist. Ein Umrüstungsnachweis kann in Form eines Fotos erbracht werden, das den Ausbau des Mikrofons dokumentiert. Ein Vernichtungsnachweis kann in der Form eines Bestätigungsschreibens einer Abfallentsorgungsstation, bei der Sie das zu vernichtende Mikrofon abgeben, erbracht werden. Auch werden hier Fotos, die eindeutig die Zerstörung des in Rede stehenden Mikrofons zeigen, als Beweis der Zerstörung zugelassen, wenn erkennbar ist, dass das Mikrofon funktionsuntüchtig ist und es sich um das in Rede stehende Mikrofon handelt.

Herrn Frank B.:

Der Tracker hatte ein kleine Notruftaste. Über diese wurden vorher einprogrammierte Telefon-Nummern automatisch angerufen. Jetzt kommt der kriminelle Akt: Durch das im Tracker verbaute Telefon konnte Herr Frank B. mit dem Angerufenen sprechen und seine Lage schildern. Ein einziger Tastendruck könnte ihm – unabhängig vom Aufenthaltsort – das Leben retten.

Herr B. fühlte sich nun sicherer, doch dieses Gefühl währte nicht lang. Im Frühjahr 2018 erhielt er einen dicken Brief von der Bundesnetzagentur. Er wurde recht barsch im altbewähren Beamtendeutsch aufgefordert den Tackert zu zerstören oder aber das Mikrophon auszubauen. Als Beleg wurde ein Foto des kastrierten Trackers gefordert.

Herr B. erhob Einspruch und bat die Bundesnetzagentur um eine Ausnahmegenehmigung wegen seiner schweren Behinderung. Monate gingen ins Land und dann kam die erhoffte Antwort. Und die war gar nicht positiv. Jetzt kam die Androhung einer Strafe von 1.000,- Euro hinzu. Das Mikrofon auslöten konnte Herr wegen seiner Behinderung nicht und es fehlte auch das technische Wissen. Und einfach rund 100,- Euro zerstören, das sah Herr B. auch nicht ein.

Die Lieferfirma – die zur Herausgabe der Kundendaten gezwungen wurde – bot Hilfe an, doch die wurde durch die Bundesnetzagentur verboten. Ein Auszug ist auf der vorherigen Seite zu sehen.

Der Anbieter PAJ nahm zu den Beschlagnahmungen (es gab viele in Deutschland) Stellung:

„Konkret stellt sich die Einstufung dass GPS Tracker von PAJ mit Mikrofon gegen TMG §90 verstoßen aus unserer Sicht wie folgt dar:
Die Bundesnetzagentur hat Ihre Einschätzung zu bestimmten Funktionen von GPS Trackern von heute auf morgen geändert. Dazu wurde die entsprechende Webseite aus der hervorgeht, wie die Bundesnetzagentur das TMG §90 aktuell interpretiert, auch erst nach einem Hinweis der Widersprüchlichkeit angepasst. Weiter werden in Deutschland aktuell noch viele GPS Tracker mit der hier angemahnten Funktion frei verkauft. Nach eigenen Aussagen ist die Bundesnetzagentur personell gar nicht in der Lage gegen alle GPS Tracker Hersteller vorzugehen und den Markt zu überwachen.

Die Entscheidung der Bundesnetzagentur zieht einen Verwaltungsprozess mit sich. Die Firma PAJ sieht sich nach der oben dargestellten Vorgehensweise der Bundesnetzagentur nicht in der Verantwortung den behördlichen Verwaltungsprozess umzusetzen. Im Zuge dessen, wurden wir verpflichtet die Lieferadressen der Geräte weiterzugeben. Ein Datenschutzgesetz greift hier nicht.

Wir sehen uns sehr wohl in der Verpflichtung unseren Kunden eine schnelle Lösung zu bieten. Dem sind wir auch nachgekommen in dem wir eine Umbauanleitung erarbeitet haben, welche beim Kunden vor Ort umgesetzt werden kann. Diese wollten wir natürlich auch nur unseren betroffenen Kunden und nicht den Mitbewerben zur Verfügung stellen. Daher sind wir an die Bundesnetzagentur herangetreten mit der Bitte, unsere Umbauanleitung dem Schreiben beizufügen.

Letztlich hatten wir hier mit unserer Vorgehensweise bezwecken wollen, dass der Kunde eine schnelle und unkomplizierte Lösung erhält um das Problem aus der Welt zu schaffen.
Wir selber waren überrascht von den harschen Formulierungen im Schreiben der Bundesnetzagentur, da sich der Verwaltungsprozess für uns aus damaliger Sicht anders dargestellte. Weiter halten wir die gewählten Fristen zur Umrüstung für zu kurz. Auch wurden wir nicht informiert, ab wann unsere Kunden ein Schreiben erhalten werden. Ein weiteres Schreiben vorab hätte unseren Kunden einfach keinen Mehrwert gebracht. Daher haben wir uns dazu entschieden, dem Kunden eine Lösung zum Problem direkt mit dem Schreiben beizufügen. Eine Information auf unserer Webseite hätte hier aus unserer Sicht auch keinem Kunden schneller zu einer Lösung verholfen....“

Übrigens: in dem Schreiben der Bundesnetzagentur lag nicht – wie versprochen – eine Umbauanleitung bei.

Ende Juli 2019 kam dann der vorläufige Höhepunkt der Geschichte. Herr B, beschrieb die Situation:

„ ...letzte Woche stand plötzlich die BNA in Gestalt zweier Kripobeamter in der Haustür mit ihren Pistolen im Holster, und traten zuerst einmal sehr martialisch auf um sich Einlass zu verschaffen. Das hätte es aber nicht wirklich gebraucht, zumal ich zur Herausgabe des fraglichen Trackers bereit war. Ich hatte das Gerät allerdings auf Anraten meines Anwaltes, nicht aktiv abgegeben um mir so die Möglichkeit zu bewahren, dem Ganzen widersprechen zu können, was bei aktiver Auslieferung und Zerstörung, oder einer von mir selber unsachgemäß durchgeführten Umrüstung die auch einer Zerstörung gleich gekommen wäre, nicht mehr zur Wahl gestanden hätte.

Aber einen Strafbefehl und einen Auftrag zur Hausdurchsuchung mit anschließender Beschlagnahme, hielt sogar der durchführende Kripobeamte für überzogen. Sogar für Bayern war das ziemlich harter Tobak. Aber egal wie es auch war, musste der Beamte seiner Pflicht Genüge tun, und hatte den Auftrag der Staatsanwaltschaft nicht zu bewerten, sondern nur umzusetzen, was er auch tat. Er empfahl mir allerdings einen Anwalt zu Rate zu ziehen...

... Es bleibt spannend. Warum meine Frau Mitbeschuldigte ist, liegt an meinem Kundenkonto bei Amazon, dass (dem Datenschutz geschuldet) auf uns beide läuft, damit ihr auch Fragen zu ausstehenden Lieferungen von Bestellungen beantwortet werden.“

Der Prozess steht noch aus. In all den vielen Monaten dieser Geschichte trieben und treiben auch deutsche Radio-Piraten im 40 Meter-Band unbehelligt von der Bundesnetzagentur ihr Unwesen und stören erheblich den internationalen Luftverkehr über dem Atlantischen Ozean.

(Siehe nächster Beitrag).

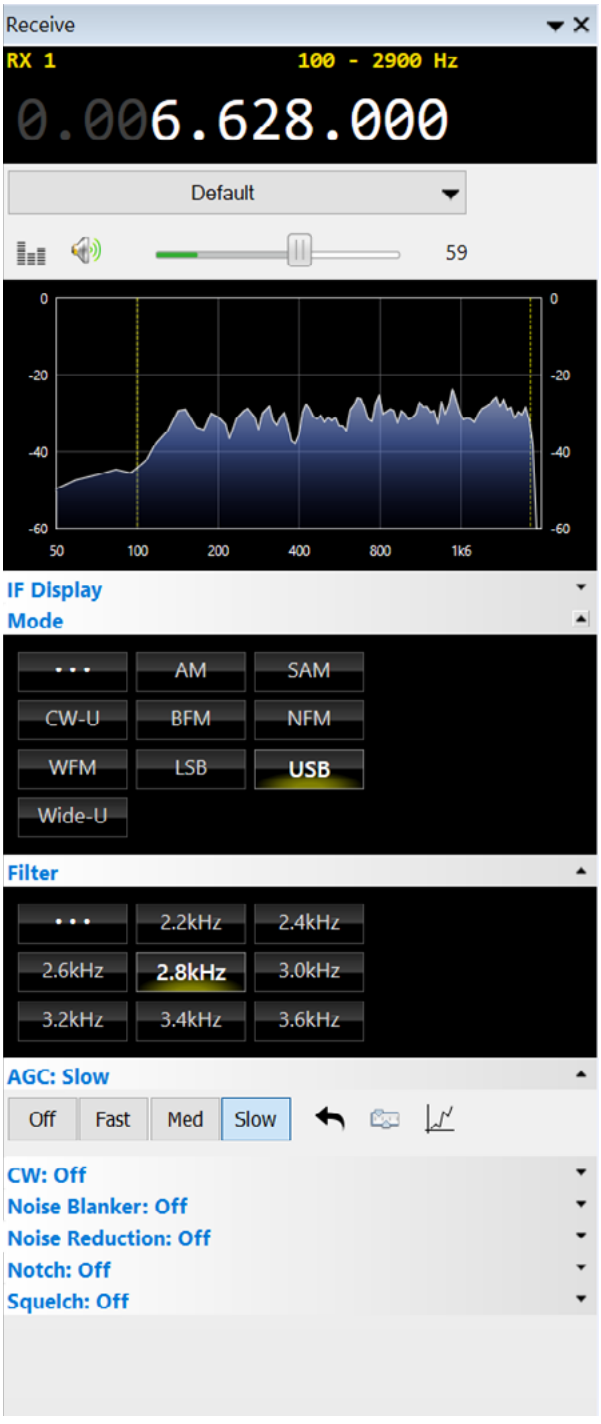
KOMMUNIKATION

„Freebander“ Nur dumm oder kriminell?

Nichts ist ruhiger als ein Nachtflug über den Atlantik aus Amerika nach Europa. In den frühen Morgenstunden reihen sich die Maschinen über dem Ozean wie auf einer Perlenschnur aneinander. Und Sie als Passagier vertrauen auf Technik und Mensch im Cockpit.

Das können Sie auch, denn die Gefahr geht von Menschen am Boden aus, die entweder kriminell oder geistig behindert sind .

Bevor wir dazu kommen, ein kleiner Einblick über die Kommunikation zwischen Flugzeugen und en Bodenstationen, die sie sicher leiten sollen. Über Land geschieht das im sogenannten VHF-Bereich zwischen 118 und 135 MHz. Diese höheren Frequenzen erlauben die Kommunikation in einem eingeschränkten Raum und sind weitgehend störsicher.

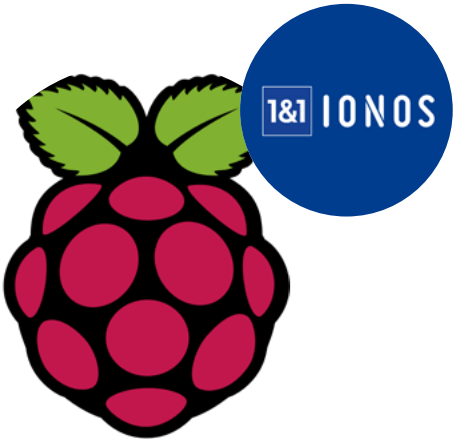


Bei Flügen über die Ozeane gibt es bei VHF ein Reichweitenproblem und da weichen dann Bodenstationen und Flugzeuge auf die Kurzwelle mit ihrer wesentlich größeren Reichweite aus. ARNIC Stationen halten die Kommunikation mit den Flugzeugen aufrecht und geleiten sie sicher über den Ozean und Volmet-Stationen versorgen die Crew mit aktuellen Wetterdaten auf der Route. Wie Autobahnen ziehen sich die sogenannten Major World Airlines Route Aereas rund um den Globus. Jeder Aerea werden bestimmte Frequenzen auf der Kurzwelle fest zugewiesen. Eigentlich eine ganz sichere Sache.

Wäre da nicht eine Gruppe von Kriminellen die sich Freebander nennen. Sie belegen genau die Frequenzbänder die der Luftfahrt zugewiesen worden sind und stören regelmäßig die Kommunikation der Piloten, die diesen illegalen Funkverkehr noch wesentlich lauter hören als wir am Boden, da sie sich im freien Raum befinden. Die sogenannten Freebander nutzen überwiegend das unters Seitenband (LSB) in der Annahme, das würde das obere Seitenband (USB) der Luftfahrt nicht stören. Doch dem ist nicht so. Die Piloten verstehen garantiert nichts mehr und die Freebander gefährden die Sicherheit der Passagiere und der Crew.

Hier ein paar Frequenzen der Nordatlantik-Route:

- Nat-b 6586 kHz, USB
- Nat-f 6622 kHz, USB
- Nat-e 6628 kHz, USB
- Mid-3 6631 kH, USBz

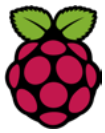


4

Eigener DNS-Server mit Raspberry Pi

So geht's

Damit Computer im Internet miteinander kommunizieren können, besitzen alle Teilnehmer im Netz eine einmalige Adresse: Durch IP-Adressen wissen Clients genau, welche Server sie ansprechen sollen. Aber kein Nutzer merkt sich die Ziffernfolgen dieser Adressen, sondern nur Domain-Namen.



Dafür ist das Domain-Name-System (DNS) da: Es wandelt Domains in Zahlen um und umgekehrt. Dazu müssen Clients erst einen oder mehrere DNS-Server anfragen, bevor sie die richtige Adresse geliefert bekommen. Das kostet mitunter wertvolle Zeit. Deshalb kann es sinnvoll sein, die Internetverbindung zu beschleunigen, indem man sich einen eigenen DNS-Server einrichtet. Ein Raspberry Pi, der kleine aber vielseitige Computer, bietet dafür eine sehr gute Basis. Wir erklären Ihnen, wie DNS funktioniert und wie Sie Ihren eigenen DNS-Server aufsetzen können.

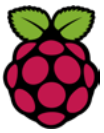
Was genau ist DNS?

Das Domain-Name-System hilft Ihnen, sich in Netzwerken, die auf IP-Adressen basieren, zurechtzufinden. In die Adresszeile Ihres Browsers geben Sie für gewöhnlich eine Domain wie www.example.org ein. Für die Kommunikation im Internet benutzen Computer allerdings IPv4- oder IPv6-Adressen. Damit die Verständigung dennoch funktioniert, muss die einprägsame Domain umgewandelt werden. Die sogenannte Namensauflösung geschieht unter Verwendung von DNS-Servern. Dafür sollte der Browser zunächst auf einen Cache zugreifen. Vielleicht ist die Adresse dem eigenen System ja bereits bekannt und muss daher gar nicht angefragt werden.

Sollte dies nicht der Fall sein, wird die Anfrage an einen oder mehrere DNS-Server weitergeleitet. Zunächst kommt hierfür meistens der DNS-Server des Internetproviders in Frage. Dieser gleicht die Anfrage mit seiner Datenbank ab und liefert im Idealfall ein Ergebnis. Wenn er keinen Eintrag für die Domain haben sollte, wird direkt bei einem der 13 Root-Nameserver des Internets nachgefragt. Dort sind alle Adressen des World Wide Webs gespeichert.

Im Zusammenhang mit DNS ist auch zu beachten, dass die meisten Teilnehmer des Internets, vor allem die Clients von gewöhnlichen Internetnutzern, keine feste IP-Adresse besitzen. Internetprovider vergeben IP-Adressen innerhalb ihres Netzes nämlich meist nur für 24 Stunden. Danach wird eine sehr kurze Zwangstrennung eingeleitet, die Internetverbindung wird dabei unterbrochen, und der Teilnehmer bekommt eine neue IP-Adresse zugewiesen. Das ist für gewöhnlich kein Problem, denn Clients werden selten von außerhalb des lokalen Netzwerks angesprochen, schließlich sind sie es, die Anfragen an Server senden – und nicht andersherum.

Für bestimmte Anwendungsfälle ist es aber notwendig, einen eigenen Server einzurichten: Remote-Desktops oder ein eigener, kleiner Gameserver beispielsweise. In solchen Fällen setzt man auf Dynamic DNS. Über einen DDNS-Anbieter bekommt der heimische Server eine Domain zugewiesen über die er durchgängig erreichbar ist. Wenn Sie also Ihren selbst gehosteten DNS-Server auch von außerhalb Ihres lokalen Netzes jederzeit ansprechen möchten, sollten Sie über DynDNS nachdenken.



Was bringt ein eigener DNS-Server?

Aus ganz unterschiedlichen Gründen greifen einige Nutzer lieber auf einen eigenen DNS-Server zurück, statt auswärts nach den IP-Adressen zu suchen. Die Einrichtung eines eigenen Servers ist besonders dann sinnvoll, wenn mehrere Geräte und Personen innerhalb des Netzwerks online gehen, z. B. in einer größeren Familie, einer WG oder auch einem kleineren Büro.

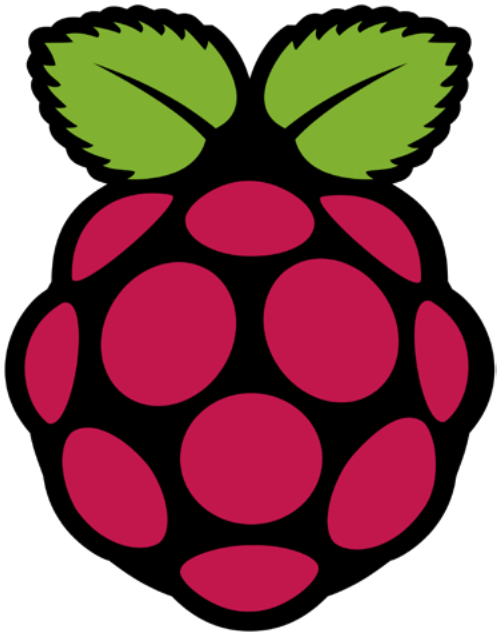
- Geschwindigkeit: Eine Webanfrage läuft – falls kein Cache-Eintrag vorhanden ist – mitunter über mehrere Router und Server, bis der Webinhalt beim Nutzer ankommt. Zwar bewegen sich diese Wartezeiten meist im Bereich von Millisekunden, aber wenn gar nicht erst eine Verbindung zum DNS-Server des Internetanbieters aufgebaut werden muss, kann der Vorgang noch beschleunigt werden.
- Privatsphäre: Damit das Domain-Name-System funktioniert, müssen die Anfragen an fremde Server weitergeleitet werden. Dabei entstehen Spuren im Internet, die manche Nutzer gerne vermeiden möchten. Mit einem eigenen DNS-Server bleiben viele Daten bei Ihnen.
- Sicherheit: Wer seinen eigenen DNS-Server hostet, hat auch die Kontrolle über die Einträge. Cyberkriminelle versuchen gerne, sich bei Anfragen an den DNS-Server des Providers dazwischen zu klinken und eine falsche IP-Adresse auszuliefern. Statt der eigentlich anvisierten Website wird dann eine andere ausgegeben. Dies ist besonders beim Onlinebanking extrem risikoreich: Werden sensible Kontodaten auf einer exakten Kopie der Bank-Website eingegeben, haben die Kriminellen schnell die Geldreserven geplündert.
- Werbefilter: Ad-Blocker greifen auf eine Liste von Werbeservern, die gesperrt werden sollen, zurück. Dies kann auch ein selbsterstellter DNS-Server leisten. Damit können Sie sogar alle Geräte in Ihrem Heimnetzwerk auf einmal von Werbeeinblendungen befreien, ohne dass Sie auf jedem Gerät extra Software installieren müssen.
- Jugendschutz: Was mit Werbung funktioniert, ist auch sinnvoll in puncto Jugendschutz. Server, die jugendgefährdende Inhalte bereitstellen, können über ein selbstverwaltetes DNS einfach geblockt werden.
- Lerneffekt: Viele Nutzer installieren ihre eigenen DNS-Server schlicht, um mehr über die Funktionsweisen des Internets zu verstehen. Strom kommt aus der Steckdose und Websites aus dem Browser: Wer aber die Technik dahinter verstehen möchte, hat mit solchen Do-it-yourself-Pro-

jekten großartige Lerneffekte – wie im Übrigen mit vielen anderen Ideen für den Raspberry Pi.

Mit Raspberry Pi einen DNS-Server einrichten

Wenn Sie auf Ihrem Raspberry Pi einen DNS-Server installieren möchten, brauchen Sie neben dem Minirechner noch:

- SD-Karte mit installiertem Rasbian
- Ethernet-Verbindung zum Internet-Router
- Stromversorgung per Micro-USB-Kabel
- SSH-Client (z. B. PuTTY)



Als Grundlage für DNS auf dem Raspberry Pi setzen wir in diesem Beispiel auf BIND. Bei BIND handelt es sich um eine Open-Source-Software, die auf den Berkeley Internet Name Domain Server zurückgeht. Inzwischen ist das Programm in seiner neunten Version vorhanden und wird vom Internet Software Consortium (ISC) weiterentwickelt.

Zunächst müssen Sie sicherstellen, dass der Raspberry Pi innerhalb des lokalen Netzwerks eine statische IP-Adresse zugewiesen bekommt. Dafür öffnen Sie die Netzwerkkonfiguration:

sudo nano /etc/network/interfaces

Dort weisen Sie dem Raspberry Pi eine einmalige IP-Adresse zu.

Tipp

Bei Nano handelt es sich um einen einfachen Linux-Editor, den Sie auf jeden Fall auf Ihrem Raspberry Pi installieren sollten.

Nun können Sie BIND installieren. Es ist sinnvoll, neben dem eigentlichen Programm bind9 auch die beiden Pakete bind9utils und dnsutils zu installieren. Diese sind zwar nicht notwendig, enthalten aber einige nützliche Werkzeuge für die Wartung Ihres neuen DNS-Servers. Wenden Sie folgenden Befehl an:

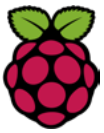
sudo apt-get install bind9 bind9utils dnsutils

Nun ist bind9 auf Ihrem System installiert. Allerdings müssen sie, bevor Sie Ihren Raspberry Pi als DNS-Server verwenden können, noch ein paar Einstellungen vornehmen. Öffnen Sie deshalb nun die Konfigurations-Datei von bind9:

sudo nano /etc/bind/named.conf.local

Dort sollten Sie nun zwei Zonen einrichten: Eine für den Forward-Lookup, bei dem die IP-Adresse zur Domain gesucht wird, und eine für den Reverse-Lookup mit der umgekehrten Fragestellung.

sudo nano /etc/bind/named.conf.local



```
zone „home.lan“ IN {
        type master;
        file „/etc/bind/db.home.lan“;
    };
zone „1.168.192.in-addr.arpa“ {
        type master;
        file „/etc/bind/
db.rev.1.168.192.in-addr.arpa“;
    };
```

Im Code ist zu erkennen, dass Sie zwei Dateien (db.home.lan und db.rev.1.168.192.in-addr.arpa) zur Definition der Zonen verwenden. Diese müssen Sie aber erst einmal erstellen. Da Sie die Dateien selbst anlegen, können Sie diese auch benennen, wie Sie möchten, müssen dies dann aber auch an allen entsprechenden Stellen so eingeben. Erstellen Sie zunächst die Datei für denForward-Lookup:

sudo nano /etc/bind/db.home.lan

```
home.lan. IN SOA raspberry.home.
lan. hostmaster.home.lan. (
     2017081401 ; serial
      8H ; refresh
      4H ; retry
      4W ; expire
      1D ; minimum
  )
  home.lan. IN NS raspberry.home.
lan.
  home.lan. IN MX 10 raspberry.
home.lan.
  localhost   IN A 127.0.0.1
  raspberry   IN A 192.168.1.31
  router      IN A 192.168.1.1
```

Die letzten beiden Einträge innerhalb der Datei müssen Sie anpassen. Geben Sie dort die IP-Adresse Ihres Raspberry Pi (dem Sie zu Anfang eine statische IP-Adresse zugewiesen haben) und die Ihres Routers ein. Achten Sie auch darauf, dass Domain-Namen hier immer mit einem Punkt abgeschlossen werden. Am Anfang der Datei, nach deren Seriennummer, legen Sie fest, wie viel Zeit zwischen regelmäßigen Aktionen liegen soll. Die beiden Angaben NS und MX (siehe MX-Record) legen fest, dass sowohl der Name-Server als auch der Mail-Server vom Raspberry Pi gestellt werden.

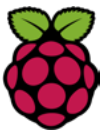
Tipp

Zu Beginn der Dateien geben Sie diesen immer eine Seriennummer: Es hat sich das Format YYYYMMDDXX eingebürgert, also das Datum (in der Reihenfolge Jahr, Monat, Tag) plus eine aufsteigende Seriennummer – falls Sie mehrere Versionen an einem Tag erstellen.

Nun erstellen Sie noch die Reverse-Zone-Datei:

**sudo nano /etc/bind/
db.rev.1.168.192.in-addr.arpa**

```
@ IN SOA raspberry.home.lan.
hostmaster.home.lan. (
     2017081401 ; serial
     8H ; refresh
     4H ; retry
     4W ; expire
```



```
    1D ; minimum
)
        IN NS raspberry.home.lan.
1       IN PTR router.home.lan.
31      IN PTR raspberry.home.lan.
```

Dieses Beispiel geht davon aus, dass Ihre lokale Netzwerkadresse mit 192.168.1. beginnt. Sollte dies nicht der Fall sein, müssen Sie den richtigen Adressraum in der Datei und dem Dateinamen definieren. Denken Sie daran, dass dann auch ein anderer Dateiname in /etc/bind/named.conf.local an entsprechender Stelle einzutragen ist.

Wenn Sie auf Ihrem Raspberry Pi einen DNS-Server installieren, fungiert dieser als Cache von DNS-Anfragen. Das heißt, sobald Sie einmal eine Namensauflösung angefragt haben, bleibt der Eintrag auf Ihrem DNS-Server gespeichert. Fürs Erste werden also DNS-Anfragen noch auf andere Server weitergeleitet. Welche Server dies sind, legen Sie in /etc/bind/named.conf.options fest. Öffnen Sie dafür die Datei und ändern Sie die IP-Adressen im Eintrag „Forwarders“:

sudo nano /etc/bind/named.conf.options

```
forwarders {
 1.2.3.4;
 5.6.7.8;
};
```

Hier tragen Sie beispielsweise die IP-Adresse des DNS-Servers Ihres Internetproviders ein oder die eines offenen Systems. Bekannt ist z. B. das Angebot von Google (8.8.8.8). Wer sich unabhängiger von kommerziellen Anbietern machen möchte, kann aber auch ein freies System wie das des Digitalcourage e. V. (85.214.20.141) wählen.

Nun haben Sie auf Ihrem Raspberry Pi den DNS-Server mit BIND konfiguriert. Damit die Änderungen wirksam werden, sollten Sie das Programm an dieser Stelle neustarten:

sudo service bind9 restart

Oder:

sudo service bind9 stop

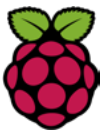
sudo service bind9 start

Falls beim Starten des DNS-Servers Fehler auftreten, lohnt es sich, einen Blick in die Logdatei unter /var/log/syslog zu werfen. Damit Sie nach einem Neustart Ihres Raspberry Pis den DNS-Server nicht erneut per Hand starten müssen, können Sie diesen in den Autostart des Systems legen:

sudo update-rc.d bind9 defaults

Nun müssen Sie nur noch Ihren neuen DNS-Server in den Einstellungen Ihres Routers eintragen, damit Anfragen zur Namenauflösung über Ihren Raspberry Pi laufen. Tragen Sie dazu in den Einstellungen des Geräts (dieses lässt sich meist über eine Weboberfläche aufrufen) die IP-Adresse des Raspberry Pi ein. Nun haben Sie Kontrolle über die DNS-Einträge und können bestimmte Server blocken, um sich beispielsweise vor Seiten zu schützen, die Ihnen schaden wollen. Dazu müssen Sie DNS-Sperren einrichten. Dies geschieht in einer Datei, die Sie zunächst in die Konfigurationsdatei von bind9 eintragen:

sudo nano /etc/bind/named.conf



Die Datei wird als neuer Eintrag unter die bereits vorhandenen eingefügt und mit einem Semikolon abgeschlossen:

include „/etc/bin/named.conf.blocked“;

In diese Datei tragen Sie nun die Domains ein, die Sie blocken möchten. Damit Sie wissen, welche Domains gesperrt werden sollen, können Sie auf verschiedene Listen zugreifen. In diesem Beispiel verwenden wir eine Liste des DNS-BH-Projekts, die eine Zone-File für BIND bereitstellen. Diese können Sie herunterladen und mit einem Texteditor öffnen. Einträge dort sind bereits im richtigen Format und können deshalb einfach in Ihre Blockliste kopiert werden. Einträge müssen – auch wenn Sie andere Quellen verwenden – dieses Format haben:

zone „malware-example.ga“ {type master; file „/etc/namedb/blockeddomain.hosts“;};

Am Ende der Zeile wird eine Datei genannt, die ausgeführt wird, wenn die entsprechende Domain aufgerufen werden soll. Diese Datei legen Sie so an:

sudo nano /etc/namedb/blockeddomain.hosts

Dort fügen Sie folgenden Code ein:

$TTL 86400

@ IN SOA raspberry.home.lan. hostmaster.home.lan. (

2017081401 ; serial

8H ; refresh

2H ; retry

10D ; expire

1D ; minimum

)

NS raspberry.home.lan.

A 127.0.0.1

*** IN A 127.0.0.1**

Achten Sie darauf, dass auch hier wieder die richtigen Werte für Ihre eigene Domain (in diesem Fall raspberry.home.lan) eingetragen sind. Starten Sie bind9 ein weiteres Mal neu. Nun sollte Ihr DNS-Server korrekt konfiguriert und startbereit sein.Formularende

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

Thorens 240-2

Im Kurztest

Viel hat sich seit 1976 im Design der Thorens-Plattenspieler nicht verändert. Genau wie damals kommt das aktuelle Modell TD 240-2 im klassischen Design daher. Verbunden mit der Verarbeitung hochwertiger Materialen. Zeitlos wirkt der schwere und stabile Echtholzkorpus.

Die Inbetriebnahme ist denkbar einfach. Transportsicherungen entfernen, Plattenteller drauf, Staubschutzhaube montieren, Anti-Skating und Auflagegewicht einstellen, anschließen und fertig. Störend wirkt die etwas billig wirkende Filzauflage auf dem Plattenteller.

Auffallend ist der Wahlschalter mit den drei Einstellungen 33, 45 und 78 Umdrehungen. Der Thorens TD 240-2 spielt mit einer optionalen Nadel tatsächlich Omas alte Schelllack-Platten mit 78 Touren ab. Wer die die Abspielautomatik bevorzugt, der kann diesem Plattenspieler vertrauen. Sanft setzt der Tonabnehmer auf der Platte auf. Natürlich geht es auch manuell.

Apropos Tonabnehmer. Der mitgelieferte AT-95E ist für einen ersten Test gut, doch auf Dauer ist die Umrüstung auf einen AT120E oder einen AT440ML vom selben Hersteller empfehlungswert. Trotz Riemenantrieb sind Gleichlaufeigenschaften hervorragend. Dafür sorgen der geschliffene Präzisionsriemen und der elektronisch geregelte Gleichstrommotor.

In der Praxis zeigte der TD 240-2 was er wirklich draufhat. Ist das Ausgangsmaterial gut, klingt nahezu jeder Plattenspieler gut. Sein wirklicher Wert zeigt sich erst bei einer mangelhaften Pressung. Bei einer Pink Floyd Platte aus deren Anfangszeit entfaltete der Thorens eine wahre Klangpracht, die manch teurerem Plattenspieler gut anstehen würde.

Der Ultra-Orthodoxe Audiophilen wird nach mehr suchen, doch der normale Nutzer mit hochqualitativen Ansprüchen wird kaum am Thorens TD 240-2 vorbeikommen. Für rund 700 Euro erhält man eine vollwertige Gegenleistung. Das zeitlose Design und die sehr gute Verarbeitung garantieren einen langen Verbleib im heimischen Wohnzimmer.


THORENS

MEDIEN

Sendeausfall

Angeblicher Cyberangriff legt rheinmaintv lahm

Der Hessische Regionalsender rheinmaintv kann schon seit Tagen kein aktuelles Programm mehr senden, auch auf der Website tut sich seit längerem nichts. Man sei Opfer eines Cyberangriffs geworden, teilte man nun via Facebook mit

Der hessische Regionalsender rheinmaintv hat schon seit Tagen mit einem längeren Sendeausfall zu kämpfen. Nachdem zunächst nur eine Störungstafel mit einem Hinweis auf technische Störungen eingeblendet worden war, läuft inzwischen wieder ein Ersatzprogramm. Auch die Website ist seit einiger Zeit nicht mehr aktuell, die neueste dort abrufbare Ausgabe der Nachrichtensendung „rheinmain im Blick“ datiert schon auf den 19. September. Via Facebook gab der Sender nun am Mittwochabend zumindest wieder ein Lebenszeichen von sich.

In einem Video erkärt man, dass man Opfer eines „sehr massiven Cyberangriffs“ geworden sei, der die gesamte technische Infrastruktur lahmgelegt habe. „Unsere Server sowie die ganzen Sendedaten funktionieren entweder nicht oder sind verschlüsselt“. Man stehe in engem Kontakt mit den zuständigen Behörden und arbeite mit Hochdruck daran, die Probleme zu beheben - das erweist sich augenscheinlich aber als recht langwieriger Prozess. Am 16. Oktober war dann rheinmaintv wieder on Air. Infos zur Lösung des Problems gab es nicht und so brodelt die Gerüchteküche immer noch.

MEDIEN

Razzia

Illegaler IPTV-Verkehr um 50% eingebrochen

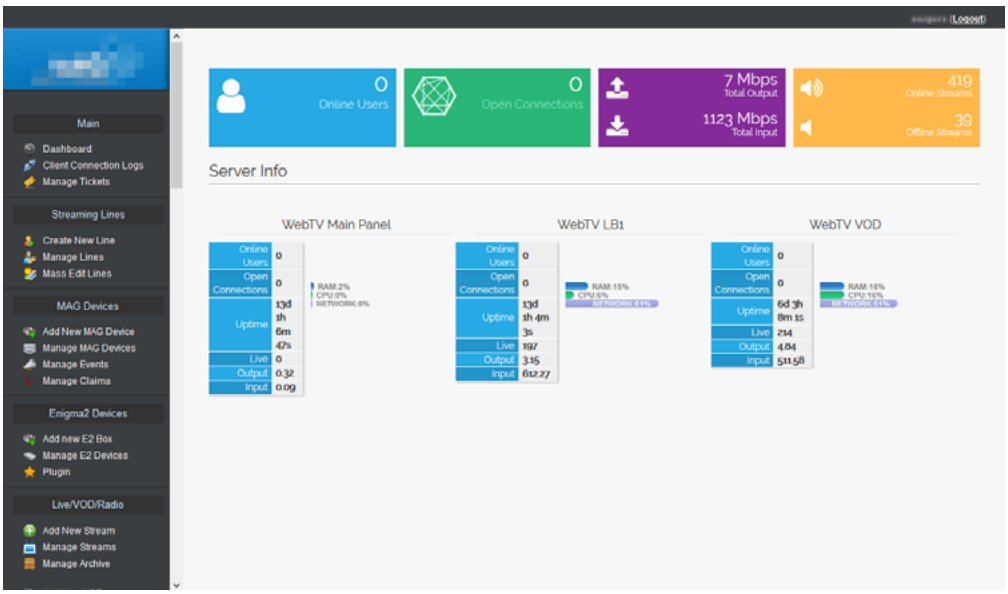
Als Xtream-Codes letzte Woche im Rahmen einer EU-Piraterie - Bekämpfung abgeschaltet wurde, herrschte Chaos. Eine große Anzahl von Diensten ging derweil offline, da der Großteil des IPTV-Marktes für die Nutzung der Software ausgelegt ist.

Illegale IPTV-Betreiber bekamen vor einigen Wochen das große Muffensausen, als die europäischen Strafverfolgungsbehörden unter italienischer Leitung zuschlugen. Nach Schätzung von TorrentFreak brach der illegale IPTV-Traffic um 50% ein.

Die Operation „Black IPTV“ nahm erst einmal italienische IPTV-Anbieter aufs Korn, die Xtream-Codes als Managementsystem nutzten. In weiteren EU-Ländern wurden die Behörden ebenfalls tätig. Direkt nach den Razzien erklärten die illegalen Anbieter, dass sie nicht mehr in der Lage seien den Betrieb fortzusetzen. Ersatz für die Xstream-Codes gab es in den ersten Tagen nicht und so verloren nicht nur die Anbieter ihre Einnahmequellen, sondern auch die illegalen Zuschauer ihren Einsatz für die Abonnements. Derzeit sind schätzungsweise 5.000 Anbietern und ca.50 Millionen Endverbraucher betroffen,

Auch wenn es keine zentrale Quelle für Informationen über den illegalen Traffic gibt, so nahm TorrentFreak einen Tag nach den Razzien Kontakt mit dem Netzwerkausrüster Sandvine auf. Sandvine hatte bereits eine detaillierte Analyse zum Piratenverkehr über das Netz erstellt. Danach bestätigte Sadvine den Rückgang dieses Traffics um ca. 50%.

Es dauerte etwa eine Woche bis einige Anbieter auf alternative Management-Systeme umsteigen konnten. Allerdings ist der Markt sehr groß und unübersichtlich und so kann heute noch nicht gesagt werden, wer wieder zurückgekehrt ist und wer nicht. Erste Abzocker nutzen die Situation für eine neue Einnahmequelle. Sie



bieten angeblich ähnliches Xstream Codes Systeme an. Nachteil? Es gibt sie nicht, die Alternative, sondern nur Gewinner, die Vorkasse für nicht existente Systeme machen.

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