Forensische Sicherung von DSL-Routern

Sebastian Braun[1] · Hans Höfken[1]
Marko Schuba[1] · Michael Breuer[2]

[1] FH Aachen

[2] Landeskriminalamt NRW
hoefken@fh-aachen.de

Zusammenfassung

DSL Router sind mittlerweile zentrale Geräte im Heimnetz. Verbindungen ins Internet, aber auch VoIP Telefoniedaten sind auf diesen Geräten abgespeichert. Die forensische Untersuchung wird jedoch erheblich durch die Vielzahl an proprietären Geräten erschwert. In diesem Paper wird versucht zu zeigen, welche Gemeinsamkeiten viele Geräte haben (sowohl beim Betriebs- und Dateisystem, als auch bei der Hardware) um darauf aufbauend ein wiederholt einsetzbares Verfahren zur Extraktion der Daten zu entwickeln.

1 Einleitung

Die Nutzung des Internets in privaten Haushalten nimmt stetig zu. Während 2003 46% der privaten Haushalte mit einem Internetanschluss versehen waren, lag diese Zahl 2013 schon bei 80,2% (vgl. [Bund]).

Um als Privathaushalt das Internet nutzen zu können, wird spezielle Hardware benötigt, meist in der Form eines DSL-Routers. Moderne DSL-Router, wie sie häufig von Internetanbietern bei Vertragsabschluss an die Kunden ausgehändigt werden, haben viele zusätzliche Funktionen jenseits des klassischen Routers. Der DSL-Router teilt den Internetzugang des Hausanschlusses mit anderen internetfähigen Geräten des Haushalts. Ein DSL-Router kann oft zusätzlich als DECT-Basisstation für schnurlose Telefone arbeiten, VoIP unterstützen oder als Medienserver agieren. Aufgrund dieser Komponenten wird in einem DSL-Router eine Vielzahl sensibler Daten, wie Telefonnummern von Kommunikationspartnern oder Dauer von Telefonaten mit diesen Partnern verarbeitet und teilweise gespeichert.

Wegen dieser Entwicklungen und der Anzahl der Daten, die von einem DSL-Router verarbeitet werden, gelangen diese Geräte immer mehr in den Fokus forensischer Untersuchungen. Mit Hilfe von gespeicherten Daten bezüglich getätigter Telefonate kann der Kontakt zu Personen nachgewiesen werden. Da die Verbindung mit dem DSL-Router über WLAN heutzutage üblich ist und mobile Geräte, wie das Smartphone, sich automatisch mit gespeicherten Verbindungen zu DSL-Routern verbinden, kann auch der Aufenthalt einer Person zu einer bestimmtem Zeit in einem Bereich um den DSL-Router festgestellt werden. Voraussetzung hierfür ist, dass der DSL-Router diese Daten speichert.

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 369-377.

Auf DSL-Routern finden sich jedoch nicht nur persönliche Daten. Mit der steigenden Anzahl von Meldungen über Angriffe auf DSL-Router werden auch sonstige Daten interessant (vgl. [Heise15a]). In der Regel stehen bei solchen Angriffen Geräte, die von größeren Internetanbietern bei Vertragsabschluss ausgeliefert werden, im Fokus(vgl. [Wisc14]). Nach der Kompromittierung werden die DSL-Router z.B. als Bot-Netz genutzt, um Folgeangriffe auf Netzwerke durchzuführen, wie es beispielsweise an Weihnachten 2014 mit den Spielenetzwerken von Sony und Microsoft geschehen ist (vgl. [Heise15b]). Eine Analyse angegriffener Router kann Hinweise auf den Täter liefern, da der Angreifer möglicherweise Spuren auf dem DSL-Router hinterlassen hat, die zum Aufenthaltsort des Täters oder zum Täter selbst führen können.

Hauptziele der hier vorgestellten Arbeit sind das Erarbeiten und die Umsetzung von allgemein gültigen Methoden zur Systemanalyse von DSL-Routern und darauf basierend die Entwicklung von Möglichkeiten zur Erstellung forensischer Sicherungen der auf den DSL-Routern gespeicherten Daten. Die Methoden sollen anschließend an einem breiten Spektrum von DSL-Routern angewendet und, zu einer Best-Practice-Anleitung zum forensischen Umgang mit DSL-Routern zur Erstellung einer Sicherung zusammengefasst werden.

2 Forensische Sicherung als Grundlage

Die forensische Sicherung von flüchtigen Daten des laufenden Systems sowie der nicht flüchtigen Daten auf den Datenträgern bilden die Grundlage einer forensischen Untersuchung. Im ersten Schritt werden von einem laufenden System die flüchtigen Daten gesichert. Dies muss unverzüglich geschehen, da diese Daten nur so lange auf dem System zu finden sind, wie dieses eingeschaltet ist und sich diese Daten zudem permanent verändern. Unter anderem lassen sich folgende Daten nur vom laufenden System sichern:

1. **Uhrzeit des Systems:** Die Uhrzeit des Systems ist relevant, um auf dem System gefundene Zeitstempel einordnen zu können. Die Uhrzeit des Systems sollte mit einer Referenzuhr verglichen werden.
2. **Inhalt des Hauptspeichers:** Im Hauptspeicher liegen Informationen bezüglich der von Prozessen verwendeten Daten sowie die Speicherbereiche, die die laufenden Prozesse belegen.
3. **Status der Netzwerkverbindungen:** Der Status der Netzwerkverbindungen gibt an, mit welchen Systemen das zu untersuchende System über ein Netzwerk verbunden ist/war. Hier sind insbesondere auch mögliche WLAN-Verbindungen interessant.
4. **Liste der laufenden Prozesse:** Diese Liste kann Aufschluss darüber geben, ob es zu den erwarteten Prozessen, weitere, eventuell verdächtige Prozesse auf dem System gibt (vgl. [Gesc14], S.88).

3 Stand der Technik

Die Untersuchung von DSL-Routern zu forensischen Zwecken ist eine noch sehr unerforschte Disziplin. Bisher wird bei forensischen Untersuchungen mit Routern hauptsächlich das Arbeitsgebiet der Netzwerkforensik erwähnt. Diese Teildisziplin beschäftigt sich jedoch vorrangig mit den Möglichkeiten der Analyse der Daten, die über ein Netzwerk versendet werden, und nicht mit denen, die darüber hinaus auf einem DSL-Router zu finden sind.

Viele DSL-Router bieten keine direkte Schnittstelle zum Extrahieren von Daten an. Bisher sind nur einige Router von Cisco dazu in der Lage. Das Auslesen dieser Router geschieht über einen

extern am Router angebrachten Konsoleneingang. Durch die Nutzung dieser Schnittstelle werden keine Daten auf dem Router verändert. Erfolgt die Datenextraktion hingegen mittels Kommunikation über das Netzwerk, werden Daten verändert. Die zum Auslesen verwendeten Befehle sind spezifisch für von Cisco fabrizierte Router. Daher funktioniert die erläuterte Vorgehensweise nur auf diesen speziellen Cisco-Routern und kann nicht als allgemeine Vorgehensweise bei der forensischen Untersuchung von DSL-Routern angewandt werden.

Internet-Recherchen (Stichworte: router forensik, router forensics) lassen in Foren und anderen Artikeln erste Ansätze zur allgemeinen DSL-Router-Forensik erkennen. Allerdings ist es auf Grund der unterschiedlichen Hard- und Software von DSL-Routern unterschiedlicher Hersteller schwierig, eine detaillierte, allgemeingültige Vorgehensweise zu erstellen.

4 Der DSL-Router

DSL-Router gehören zur Kategorie der eingebetteten Systeme. Eingebettete Systeme sind ein Bestandteil eines technischen Systems und steuern oder regeln Prozesse oder Komponenten dieses Systems (vgl. [Eign12], S. 4). Der Aufbau eines eingebetteten Systems ist seinem Zweck angepasst und deshalb nicht so komplex wie der eines PCs. Moderne DSL-Router, wie sie im Rahmen dieser Arbeit untersucht wurden, besitzen einen größeren Funktionsumfang als klassische Router. Folgende Komponenten sind häufig in moderne DSL-Router integriert:

- DSL-Modem
- WLAN-Modul
- DECT-Basisstation
- VoIP-Funktion

Durch diese zusätzlichen Komponenten verarbeiten moderne Router eine große Menge von Informationen.

4.1 Forensisch relevante Hardwarekomponenten

Durch den hohen Funktionsumfang, den moderne DSL-Router bieten, sind in ihnen viele verschiedene Hardwarekomponenten verbaut. Für die hier vorgestellte Vorgehensweise sind nur drei relevant: das System-on-a-Chip (SoC) Modul, der Arbeitsspeicher und der Flash-Speicher.

Ein *System-on-a-Chip* ist ein einzelner Chip, auf dem sämtliche für ein System benötigte Bestandteile angebracht sind, wie Mikroprozessor, Bussystem, Schnittstelle zum externen Speicher, Modul zur Kontrolle des direkten Speicherzugriffs auf den externen Speicher, Speicher für Boot-Code, Interrupt-Controller und Phasenregelschleife. Der *Arbeitsspeicher* ist der flüchtige Hauptspeicher des Routers. Der *Flash-Speicher* ist das permanente Speichermedium. Dort gespeicherte Daten gehen bei Stromverlust nicht verloren.

4.2 Forensisch relevante Softwarekomponenten

Damit ein DSL-Router forensisch untersucht werden kann, ist es relevant zu wissen, aus welchen Software-Komponenten das System besteht und welche Funktionen diese bereitstellen.

Aus dem Wissen über die Software ergeben sich forensische Untersuchungsmöglichkeiten. Die für diese Arbeit relevanten Komponenten sind der *Bootloader* und das *Betriebssystem*. Der Großteil der untersuchten DSL-Router verwenden *Embedded Linux* als Betriebssystem.

5 Kommunikation mit dem DSL-Router

Zur Sicherung der Daten des DSL-Routers wird eine Möglichkeit benötigt, mit diesem zu kommunizieren.

5.1 Schnittstellen UART und Telnet

Jeder im Rahmen dieser Arbeit untersuchte Router bietet die Möglichkeit der Verbindung über eine *UART*-Schnittstelle (UART – Universal Asynchronous Receiver Transmitter). Wenige der untersuchten Router lassen sich über Telnet ansprechen.

UART ist die Bezeichnung für eine serielle Schnittstelle. Diese ermöglicht eine Vollduplex-Kommunikation mit einem anderen Gerät, zum Beispiel dem Computer. Die grundlegende Kommunikation dieser Schnittstelle erfolgt über zwei Kanäle. TxD dient zum Senden von Daten, RxD zum Empfangen.

Telnet ist ein Protokoll, das die Möglichkeit bietet, sich über ein Netzwerk auf entfernten Rechnern anzumelden und mit diesen zu kommunizieren. Es wird auf einigen DLS-Routern als Dienst angeboten.

5.2 Die Hardware-Debugschnittstelle JTAG

Eine weitere Möglichkeit der Erstellung forensischer Sicherung ist die Hardware-Debugschnittstelle JTAG. JTAG wurde ursprünglich aufgrund der zunehmenden Verkleinerung von Hardwarekomponenten zur automatisierten Prüfung von Hardware auf Platinen entwickelt.

Oft sind in Geräten mehrere Hardwarekomponenten verbaut, die eine JTAG- Schnittstelle bereitstellen. Es ist nicht notwendig, die Schnittstelle des anzusprechenden Bauteils zu bestimmen, da sämtliche JTAG-fähigen Komponenten zu einer sogenannten Scan-Chain verbunden sind. Über diese Scan-Chain lassen sich sämtliche Komponenten über einen JTAG-Anschluss ansprechen. Mit Hilfe von JTAG lassen sich nicht nur die in der Scan-Chain befindlichen Komponenten manipulieren. Ist eine dieser Komponenten beispielsweise mit dem Flash-Speicher verbunden, lässt sich auch dieser über die JTAG-Schnittstelle auslesen und beschreiben.

5.3 Chip-Off

Bei einem Chip-Off wird der Flash-Speicher aus dem DSL-Router entfernt, mit einem speziellen Adapter verbunden und mit einem für den Chip passenden Programm ausgelesen.

6 Methoden zur Analyse der DSL-Router

Im Folgenden werden die verwendeten Methoden der Analyse näher betrachtet. Um die beschriebenen Methoden durchzuführen, wurde folgender Versuchsaufbau verwendet: an einen USB-Anschluss des Untersuchungscomputers ist ein FTDI-Chip angeschlossen. Durch diesen Chip kann der Computer über einen USB-Anschluss mit der UART-Schnittstelle kommunizieren (vgl. [FTDI]). An den FTDI Chip ist ebenfalls die UART-Schnittstelle des DSL-Routers angeschlossen. Es müssen die benutzten Anschlussmöglichkeiten beim DSL-Router hergestellt werden, die teilweise durch Anlöten von entsprechenden Verbindungen auf der Platine des Gerätes erreicht werden. Dazu muss das Gerät geöffnet und die passenden Kontakte müssen ermittelt werden. Teilweise sind die Kontakte beschriftet, manchmal können sie nur durch Ausprobieren gefunden werden.

6.1 Bootloaderanalyse

Die Bootloaderanalyse ist in zwei Bereiche unterteilt: die Analyse der während des Bootvorgangs erzeugten Ausgabe sowie das Überprüfen der Möglichkeiten durch die Benutzerschnittstelle. Die während des Bootvorgangs vom DSL-Router erzeugte Ausgabe enthält einige für die Systemanalyse relevante Informationen, wie z.B.:

- Bezeichnung und Version des Bootloaders,
- Bezeichnung, Größe und Partitionierung der/des integrierten Flash-Speicher/s,
- Bezeichnung und Größe des Arbeitsspeichers,
- Bezeichnung des SoC oder der im SoC integrierten CPU,
- Bezeichnung des verwendeten Kernels und
- Bezeichnung des verwendeten Betriebssystems.

Durch das Wissen über den verwendeten Bootloader kann eingeschränkt auf den verwendeten SoC geschlossen werden, falls dieser verdeckt ist, da manche Bootloader speziell für bestimmte SoC hergestellt wurden (vgl. [Lich06], S. 1). Durch die Betriebssystemversion kann wiederum auf Informationen wie die Version eines verwendeten Dateisystems geschlossen werden.

6.2 Betriebssystemanalyse

Bei der Betriebssystemanalyse wird geprüft, welche Möglichkeiten der Untersuchung das Betriebssystem liefert. Auch das verwendete Dateisystem kann über diese Analyse ermittelte werden. Die in dieser Arbeit verwendeten Router konnten mit Hilfe des Betriebssystems nur untersucht werden, wenn dieses eine Shell zur Verfügung stellt. Die Kommunikation mit dem DSL-Router erfolgte dabei über die UART-Schnittstelle.

7 Forensische Sicherung bei DSL-Routern

Forensische Sicherungen, aus denen gerichtsverwertbare, digitale Beweise extrahiert werden, unterliegen strengen Anforderungen. Die in dieser Arbeit verwendeten Sicherungsmethoden für DSL-Router erfüllen diese Anforderungen für die Sicherung von Arbeits- und Flash-Speicher und werden im Folgenden näher betrachtet.

7.1 Das Unix-Tool dd

Das nicht-kommerzielle Tool dd zum Erstellen von forensischen Duplikaten (vgl. [Jone11], S. 187) gehört zu den Hauptwerkzeugen, die während einer forensischen Untersuchung verwendet werden. Durch die hohe Flexibilität ermöglicht dd das Duplizieren fast jedes Datenträgers.

7.2 Sicherung mit Hilfe des Bootloaders

Nicht jeder Bootloader unterstützt die Möglichkeit der Sicherung, da bei modular aufgebauten Bootloadern Befehle vom Hersteller des Routers entfernt werden können. Dies ist nur durch Testen herauszufinden.

In einigen Fällen unterstützen Bootloader die Möglichkeit, den Inhalt des integrierten Flash-Speichers auf einer Konsole byteweise auszugeben, die dann gespeichert werden können.

Da bei dieser Methode der Router neu gestartet werden muss, kann der Arbeitsspeicher dann nicht gesichert werden.

8 Anfertigen von forensischen Sicherungen

Im Rahmen dieser Arbeit wurden forensische Sicherungen mit Hilfe des Programms *dd* und mit Hilfe des Bootloaders erstellt. Dies sind die einfachsten Möglichkeiten eine Sicherung zu erstellen. Erst wenn diese Möglichkeiten nicht gegeben sind, können die aufwändigeren JTAG und Chip-Off Methoden eingesetzt werden.

Es wurden folgende populäre DSL-Router untersucht:

- Linksys WAG320N
- Vodafone EasyBox 803A
- TP-Link TD-W8960NB
- Fritz!Box 7272
- Netgear DGND3800B
- Samsung SMT-G3010
- D-Link DVA G3342SD
- Telekom Speedport W723V Typ A
- Telekom Speedport W504V Typ A
- Telekom Speedport W700V
- Targa WR500 WoIP
- O2Box 6431

Dabei wurde wie vorher beschrieben vorgegangen:

- **Vorbereitung:** Welche Schnittstellen stellt der DSL-Router zur Verfügung?
- **Hardwareanalyse:** Welche Hardwarekomponenten sind auf dem Motherboard identifizierbar?
- **Bootloaderanalyse:** Welche (evtl. bekannten) Bootloader kommen zum Einsatz?
- **Betriebssystemanalyse:** Welches Betriebssystem wird verwendet, welche Programme sind dadurch verfügbar?

Aus dieser Vorgehensweise wurde ein Best-Practice erstellt, das auch bei anderen Routermodellen zum Einsatz kommen kann.

9 Best-Practice

Muss ein DSL-Router im Zuge einer Ermittlung untersucht werden, ist folgende Vorgehensweise empfehlenswert, um möglichst viele Daten zu sichern. Vorausgesetzt ist, dass bei Bedarf nach dem Vier-Augen-Prinzip gehandelt und Software mit Dokumentationsfunktion verwendet wird, um gefundene Daten gerichtsverwertbar nutzen zu können.

Ist der DSL-Router noch eingeschaltet, lassen sich möglicherweise relevante, flüchtige Daten, die beim Ausschalten des Gerätes verloren gehen, noch sichern. Zu diesen Daten können Zeit

und Datum des Gerätes, aktive Netzwerkverbindungen und Inhalt des Arbeitsspeichers gehören. Somit ist mit größter Vorsicht vorzugehen, damit das Gerät nicht versehentlich ausgeschaltet wird.

Zunächst muss der DSL-Router geöffnet werden. Sind die Schrauben, die den DSL-Router geschlossen halten, nicht direkt zu sehen, liegen diese möglicherweise unter den Gummifüßen. Ist der DSL-Router geöffnet, muss die UART-Schnittstelle lokalisiert werden. Ist diese gefunden, müssen die einzelnen Kontaktpunkte richtig besetzt werden. Bei falscher Besetzung ist keine Kommunikation mit dem Gerät möglich. Ist der DSL-Router mit dem Untersuchungscomputer verbunden, und die Kommunikationssoftware aktiv, kann mittels Tastendruck herausgefunden werden, ob das Betriebssystem über eine Shell verfügt. Benötigt die Shell zur Aktivierung Login-Daten, können diese eventuell recherchiert oder bekannte Standard-Login-Daten ausprobiert werden. Es besteht ebenfalls die Möglichkeit, dass diese Login-Daten vom Besitzer des Routers selbst gewählt wurden. Diese können nur durch Erraten oder Kooperation des Besitzers ermittelt werden.

Ist eine Shell verfügbar, sollte geprüft werden, welche Befehle zur Verfügung stehen. Ist der zur Verfügung stehende Befehlssatz bekannt, können mit Hilfe dieser Befehle zunächst die flüchtigen Daten gesichert werden. Zur Sicherung des Arbeitsspeichers und des Flash-Speichers ist meist ein externes Speichermedium notwendig. Um dies verwenden zu können, muss der DSL-Router eine Möglichkeit bieten, zum Beispiel über eine USB-Schnittstelle, ein Speichermedium anzuschließen. Ist ein Speichermedium angeschlossen und Befehle zur Sicherung verfügbar, kann der Arbeitsspeicher und Flash-Speicher gesichert werden. Teilweise verfügen die DSL-Router über keine USB-Schnittstelle oder stellen keinen Befehl zur direkten Sicherung zur Verfügung. Nun ist zu testen, ob die Shell einen Befehl zur Darstellung des Inhaltes der internen Speichermedien auf der Konsole zur Verfügung stellt. Diese Ausgabe kann geparst und in eine Datei geleitet werden.

In Ausnahmefällen kann es sein, dass der DSL-Router, obwohl er über eine USB-Schnittstelle verfügt und nötige Befehle zur Sicherung bereitstellt, keine Sicherung zulässt (z.B.: OpenWRT, dd-wrt).

Stellt der DSL-Router keine Shell mittels UART-Schnittstelle zur Verfügung, kann geprüft werden, ob dies über Telnet möglich ist. Hierbei ist zu beachten, dass die Kommunikation mittels Telnet den Status des Routers stark verändert, da ein Gerät in das Netzwerk eingebunden wird. Dies muss genau dokumentiert werden.

Ist eine Sicherung mittels Shell nicht möglich, gilt es zu prüfen, ob eine Sicherung mit Hilfe des Bootloaders möglich ist. Da dafür das Gerät neu gestartet werden muss, gehen die flüchtigen Daten verloren. Stellt der Bootloader einen Befehl zur Sicherung zur Verfügung, kann diese erfolgen.

Als nächste mögliche Sicherungsoption sollte geprüft werden, ob der DSL-Router über eine JTAG-Schnittstelle verfügt. Ist diese Art der Sicherung ebenfalls nicht möglich, bleibt der Chip-Off als letzte Option. Die Gefahr beim Chip-Off liegt in der potentiellen Zerstörung des Flash-Speichers, wodurch sämtliche digitalen Beweise vernichtet werden. Der DSL-Router ist nach einem Chip-Off zerstört.

Durch vorherige Ermittlung der Sicherungsmöglichkeiten eines DSL-Router-Modells kann der Vorgang der Sicherung beschleunigt werden, da bekannt ist, welche Optionen der DSL-Router zur Verfügung stellt. Die Überprüfung, ob eine Shell mittels UART oder Telnet zur Verfügung

gestellt wird, sollte jedoch immer geprüft werden, da mittlerweile mehrere Open-Source-Projekte bestehen2, die beschreiben, wie ein anderes, meist auf Linux basierendes Betriebssystem, auf einem DSL-Router installiert werden kann.

10 Ausblick

Mit dieser Arbeit wurde nur die Grundlage für eine forensische Untersuchung von DSL-Routern geschaffen. Um diese komplett analysieren zu können, bleiben noch einige offene Punkte.

Die Daten der Sicherungen müssen verfügbar gemacht werden. Die Hersteller verwenden häufig ältere oder selbst veränderte Dateisysteme für die Partitionen. Die Sicherungen müssen analysiert und eine Möglichkeit geschaffen werden, die Dateisysteme zu entpacken. Ein weiteres Problem liegt in verschlüsselten Partitionen. Speichert der DSL-Router die Daten verschlüsselt ab, kann es teilweise unmöglich sein, diese zur Verfügung zu stellen. Mittels Reverse-Engineering könnte die Verschlüsselung analysiert und evtl. gebrochen werden. Sind diese Daten verfügbar, kann mit der weiteren forensischen Untersuchung fortgefahren werden.

Dann gilt es, die Daten zu interpretieren. Es muss ermittelt werden, wo welche relevanten Daten gespeichert werden und wie diese zu interpretieren sind. Die Schwierigkeit besteht vor allem darin, dass jeder Hersteller die Daten anders auf den Geräten ablegt, beziehungsweise auch große Unterschiede bei verschiedenen Modellen eines gleichen Herstellers existieren können.

Literatur

[Bund] Statistisches Bundesamt. Ausstattung privater Haushalte Informations- und Kommunikationstechnik – Deutschland, https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html (Stand:11.03.2015).

[Eign12] M. Eigner, Torsten Gilz, Florian Gerhardt, und Fabrice Mogo Nem. Informationstechnologie für Ingenieure. 2012.

[FTDI] FTDI. http://www.ftdichip.com/FTCorporate.htm (Stand: 06.01.2015).

[Gesc14] A. Geschonneck. Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären. dpunkt.verlag, 6. Auflage, 2014.

[Heise15a] heise Security. Asus-Router schutzlos bei Angriffen aus dem eigenen Netz, http://www.heise.de/security/meldung/Asus-Router-schutzlos-bei-Angriffen-aus-dem-eigenen-Netz-2515120.html, 09.01.2015.

[Heise15b] heise Security. Gehackte Router als Bot-Netz, http://www.heise.de/security/meldung/Gehackte-Router-als-Bot-Netz-2515682.html, 11.01.2015.

[Jone11] K.J. Jones, R. Bejtlich, C.W. Rose. Real Digital Forensics: Computer Security and Incident Response. Addison-Wesley, 2011.

[Lich06] M. Lichtenberg. Common Firmware Environment (CFE): Functional Specication. 2006.

[Wisc14] D. Wischnjak. Immer Ärger mit der EasyBox, http://www.heise.de/security/artikel/Immer-Aerger-mit-der-EasyBox-2294914.html, 06.12.2014.

Anhang: Übersicht aller Router – Ergebnisse

Modell	SoC	Flash Speicher	RAM	Shell	Bootloader-UI	BS	JTAG	USB	dd-Sicherung	Boot-loader Sicherung	Tel-net	Anmerkungen
Linksys WAG320N	Broadcom BCM6358 *	MXIC MX29LV640E BTI-70G	Etrontech EM6AA160TS A-5G	Ja	Ja (CFE 1.0.7-102.1)	Linux 2.6.21.5	Nein	Ja	Ja	Ja	Nein	\
Vodafone EasyBox 803 A	/	MXIC MX29LV640BB*	Zentel A4S12D40FTP-G5	Nein	Ja(DANUBE 1.04.01)	\	Nein	Nein	Nein	Ja	Nein	\
TP-Link TDW8960NB	Broadcom BCM6358	Spansion FL032PIF	Zentel A3S56D40FTP-G5	Ja (sh für vollen Umfang)	Ja (CFE 1.0.37-102.9)	Linux 2.6.21.5	Ja	Nein	Nein	Ja	Ja	Shell-Login: admin/admin oder user/user;
FritzlBox 7272	/	Micron 29F1G08ABA DAWP MXIC MX25L8035E	/	Ja	Ja (EVA 2823)	Linux 2.6.32.60	Ja	Ja	Ja	Ja	Nein	Keine gültige Adresse für Bootloadersicherung gefunden
Netgear DGND3800B	Broadcom BCM6368 *	Spansion S34ML01G100 TFI000 Spansion S29GL256S90 TFI010	Samsung K4H511638JLCCC	Ja	Ja (CFE 1.0.37-104.4)	Linux 2.6.21.5	Ja	Ja	Nein	Ja	Nein	\
Samsung SMTG3010	/	/	/	Ja	Nein	Linux 2.40.20-AMAZON-3.1.5	/	Ja	/	Nein	Nein	Shell-Login unbekannt
D-Link DVAG3342SD	/	/	/	Ja	Ja (Amazon 1.0.0)	Linux 2.4.31-AMAZON-3.2	Nein	Ja	Nein	Nein	Nein	dd Befehl verfügbar, jedoch USB-Stick über Shell nicht ansprechbar
Telekom Speedport W 723V Typ A	Broadcom BCM 6368*	AMD AM29LV320MT*	Etrontech EM6AA160TSA-5G	Nein	Nein (CFE 1.0.37-102.6)	/	Nein	Nein	Nein	Nein	Nein	Bootvorgang lässt sich nicht unterbrechen
Telekom Speedport W 504V Typ A	/	MXIC MX29LV640E BTI-70G	Zentel A3S12D40ETP	Nein	Ja (DANUBE Loader 1.01.06)	/	Nein	Nein	Nein	Ja	Nein	Bootloader-UI Password: erste 4 Stellen des Gerätepasswortes
Telekom Speedport W 700V	/	/	PSC AS2V28S40CTP	Nein	Nein	/	Nein	Nein	Nein	Nein	Nein	Keine Bootloaderausgabe
Targa WR500 VoIP	Broadcom BCM 6341	/	/	Ja (sh für vollen Umfang)	Ja (CFE 1.0.37-0.6)	Linux 2.6.8.1	Nein	Nein	Nein	Nein	Nein	Shell-Login: admin/0000; dumpmem des BS zur Sicherung
O2Box 6431	/	EON EN29LV640L*	Etrontech EM68B6CWQ D-25H	Nein	Ja(DANUBE Loader 1.07.07)	/	Nein	Nein	Nein	Ja	Nein	Configuration Partition verschlüsselt

Legende: * : Angabe der Bootloaderausgabe entnommen, / : Angabe unbekannt