**Inhaltsverzeichnis**

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

# Abstract

# Zusammenfassung

**Kapitel 1**

**Einleitung**

* 1. **Ausgangslage**

Das Internet wird ein zunehmend wichtigerer Teil des menschlichen Lebens. Öffentliche Hotspots, Internet fähige Alltags-Geräte (IOT-Geräte) und mobiles Arbeiten von Zuhause sind nur einige Beispiele für technologische Neuerungen, welche ohne das Internet nicht möglich wären. Die rund 35,5 Mio. Netzanbindung an DSL-, Kabel-, oder Glasfaser-Anschlüsse in Deutschland [SOURCE] werden in Heimnetzen und Kleinunternehmen überwiegend durch Netzwerkrouter realisiert. In vielen Fällen bildet der Router die direkte Schnittstelle zwischen dem Internet und dem privaten Netzwerk. So stellt dieser meist auch die einzige zentrale Sicherheitskomponente zum Schutz des Netzwerkes bereit. Ein erfolgreicher Angriff auf den Router bietet einem Angreifer unzählige Möglichkeiten in das Netz einzugreifen und so immensen Schaden anzurichten. Neben bekannten Zielen wie private Daten und Passwörtern kann der Router auch als Teil eines Bot-Netzwerks für Distributed Denial-of-Service (DDoS) verwendet werden [SOURCE] oder als Einfallstor auf weitere Geräte des Netzwerkes [SOURCE]. Die Korrelation mit stark steigenden Fällen von Cyberkriminalität [SOURCE LAGEBERICHT] zeigt wie wichtig ein inhärent geschützter Router mit sicherer Konfiguration ist.   
 Handelsübliche Router wie sie in Privathaushalten und Small Office, Home Office (SoHo) Umgebungen eingesetzt werden sind bereits mit einem proprietären Betriebssystem bespielt. Die Sicherheit dieser Distribution kann also nur mit großem Aufwand von Endnutzern verifiziert werden, sowie Sicherheitsupdates nur vom Hersteller veröffentlicht werden. Hersteller können in der zunehmend kürzer werdenden Zeit zwischen neuen Iterationen von Malware meist nicht in einer angemessenen Zeit reagieren, um Sicherheitsupdates zur Verfügung zu stellen. Quelloffene Router Firmware wie OpenWrt, DD-Wrt, Tomato oder LibreCMC bieten eine Alternative zu den vorinstallierten, proprietären Betriebssystemen der Router. Diese Projekte können vollständig eingesehen, modifiziert und kompiliert werden, sodass die Sicherheit des Produktes einfach evaluiert werden kann. Ebenfalls können aufgrund der hohen Zahl an Mitwirkenden Sicherheits- und Funktionsupdates schneller entwickelt und veröffentlicht werden. Umfangreiche Überprüfungen dieser Projekte, wie z.B. anhand der BSI TR-03148: Sichere Broadband Router, werden allerdings aufgrund des hohen Zeit- bzw. Kosten- Aufwands selten durchgeführt, sodass diese auch eine Zertifizierung nicht erlangen können. Eine solche Zertifizierung könnte ungeschulten Endnutzern auch diese quelloffenen Router-Betriebssysteme als Alternativen näherbringen und somit zu einem höheren Sicherheitsniveau in privater und SOHO Netzwerkinfrastruktur führen.

* 1. **Was ist OpenWrt?**

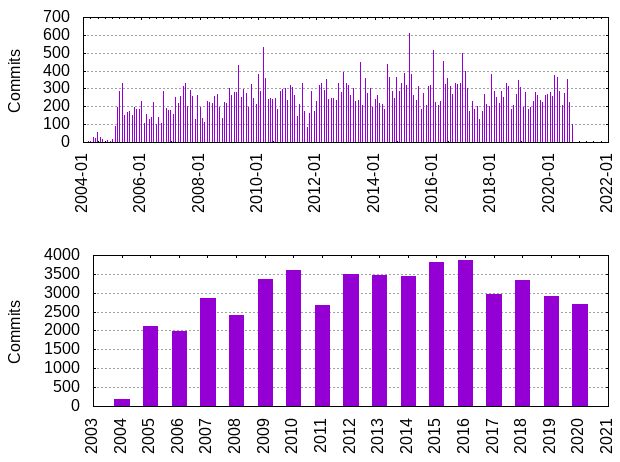
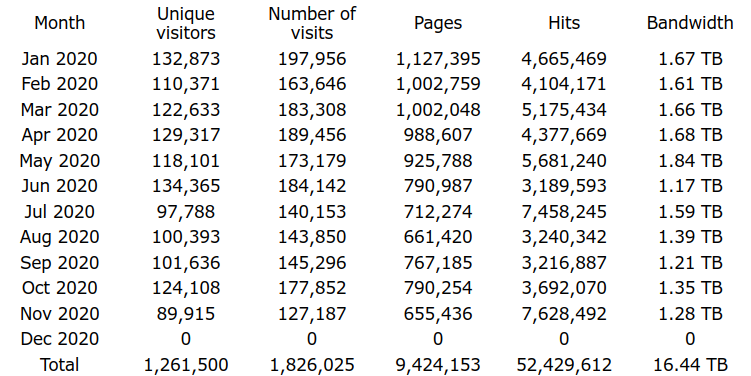
OpenWrt (**Open** **W**ireless **R**ou**T**er) ist ein quelloffenes Netzwerk-Betriebssystem für Router, welches auf GNU/Linux basiert und durch eine GNU General Public License (GPL) lizensiert ist. Die Installation umfasst einen bootloader, kernel, ein eigenes Dateisystem und ausgewählte Anwendungen. Es kann auf Routern, Switches und Accesspoints eingesetzt werden, um die vorinstallierte Firmware zu ersetzen. Es bietet neben standardmäßiger Router Funktionalität einen eigenen Paketmanager, über welchen ca. 3800 (Stand 01.11.20) weitere Pakete installiert werden können [Source]. Dies bietet viele weitere Einsatzmöglichkeiten und Funktionen, welche vom Hersteller nicht oder unzureichend unterstützt werden. Ebenfalls wird OpenWrt mit BusyBox, einem SSH Dienst, und Luci, einem Web-Interface, ausgeliefert, sodass der Nutzer vollständigen Zugriff auf das Gerät hat. Nach derzeitigem Stand werden über 1700 Geräte von ca. 270 Herstellern von OpenWrt unterstützt [Source]. Diese Anzahl Geräte kann unter anderem deshalb unterstützt werden, da OpenWrt nur minimale Ressourcen auf dem Endgerät benötigt. Nach eigenen Angaben kann die derzeitige Version, mit Einschränkungen, auf Geräten installiert werden, welche 4MB Flash Speicher und 32MB RAM besitzen. Ab der nächsten Version werden 8MB Flash und 64MB RAM vorausgesetzt [Source]. Diese Vorrausetzungen sind jedoch bei den meisten Geräten der letzten Jahre gegeben [Source].  
OpenWrt zeichnet sich ebenfalls dadurch aus, dass es sich nicht nur um eine statische Firmware handelt, sondern ebenfalls um ein komplettes Framework um angepasste Firmware Versionen zu erstellen. Ebenfalls zeichnet sich OpenWrt dadurch aus, dass Geräte solange unterstützt werden, wie sie diese Grundanforderungen erfüllen. Dies steht im Gegensatz zu den meisten proprietären Betriebssystemen, welche nur einige Jahre lang Funktions- und Sicherheitsupdates erhalten und nach ihrem sog. „End of Life“ (EOL) nicht mehr sicher betrieben werden können und ausgetauscht werden müssen. Auch wenn in der Entwicklungsgeschichte von OpenWrt viel für die Benutzerfreundlichkeit des Betriebssystems getan wurde ist es jedoch nicht für Laien geeignet. Auch wenn das Management rein über die Weboberfläche geschehen kann, erweist sich die Einrichtung ohne Grundkenntnisse als schwierig.   
 Die Entwicklung von OpenWrt begann 2004, nachdem der amerikanische Hersteller Linksys zuvor einen Router auf den Markt brachte, dessen Firmware ebenfalls unter der GPL Lizenz stand und somit öffentlich verfügbar sein musste. Die erste Veröffentlichung von OpenWrt erfolgte im Januar 2006 mit Version 0.9 (White Russian). Seitdem wurde das Projekt stetig weiterentwickelt (siehe Abbildung 1). 2016 spaltete sich eine Gruppe Mitwirkender aufgrund interner Diskrepanzen ab und gründete das LEDE Projekt. Jedoch wurde LEDE bereits 2018 wieder in OpenWrt integriert, sodass beide Projekte nun wieder zusammen unter einem Namen entwickelt werden. Die derzeit aktuelle Version ist 19.07.4, welche am 10.09.2020 veröffentlicht wurde.

Abbildung : Git commits pro Monat und pro Jahr. Die Datenreihe beginnt am 28.03.2004 und endet am 25.10.2020

* 1. **Relevanz und Verwendung von OpenWrt**

Die Webseite des OpenWrt Projektes verzeichnete im Jahre 2020 bis einschließlich November 1.261.500 einzigartige Besucher, sowie 52,4 Millionen Seitenaufrufe. Insgesamt wurden bereits 16,44TB Daten abgerufen [Source]. Die aktuelle Version von OpenWrt, 19.07.4, wurde dabei alleine im November 1981 Mal heruntergeladen. Ebenfalls wurde Version 18.06.8 noch 935 Mal angefragt. Zusammen wurden ca. 10000 Firmware-Abbilder im November heruntergeladen [Anhang]. Wie die Daten zeigen ist OpenWrt keinesfalls ein kleines Projekt mit nur wenigen Interessierten, sondern eine nachgefragt Alternative für Heimrouter, Unternehmen und Entwickler. Es lässt sich nur schwer abschätzen wie die Verteilung zwischen dem privaten und wirtschaftlichen Einsatz der Firmware ist, jedoch ist eine mehrheitliche Nutzung im privaten Umfeld zu vermuten. OpenWrt ist nicht nur für Heimrouter relevant, sondern zeichnet sich auch in seinem Nutzen für Unternehmen und Entwickler aus. Es bietet Unternehmen die Möglichkeit ein Netz zu betreiben, welches sie vollständig mit quelloffener Software realisieren und steuern können. Ebenfalls bietet es Dienstleisterunternehmen einen Weg hochgradig maßgeschneiderte Netzstrukturen für ihre Kunden zu entwerfen, welche quelloffen und leicht anpassbar sind. So können neue oder geänderten Funktionen über ein Paket bereitgestellt und verteilt werden.

* 1. **Beschreibung der BSI TR-03148**

Bei der Technischen Richtlinie „Sichere Breitband Router“ (BSI TR-03148) des Bundesamtes für Sicherheit in der Informationstechnik handelt es sich um eine Sammlung von grundlegenden Sicherheitsanforderungen für Breitband Router. Der Schwerpunkt der Richtlinie liegt hierbei auf Heimroutern, sowie auf Geräten, welche im sogenannten SOHO (Small Office, Home Office) Umfeld eingesetzt werden. Das Dokument wird durch die Dokumente „BSI TR-03148 Implementation Conformance Statement (ICS)“ sowie „BSI-TR-03148-P ICS and Test Documentation” ergänzt. In diesen Dokumenten sind Testfälle und Dokumentation zur Durchführung einer Prüfung festgehalten. Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik richtet sich die Technische Richtlinie vor Allem an Hersteller von Routern, sie kann jedoch auch für Endnutzer relevant sein, wenn diese einen neuen Router anschaffen möchten und sich im Zuge dessen über den Stand der Technik informieren wollen [SOURCE]. Es werden Anforderungen für ein Mindestmaß an verpflichtenden und einigen optionalen IT-Sicherheitsmaßnahmen definiert, um ein grundlegendes Niveau für die Sicherheit dieser Geräte zu schaffen [Source].   
 Das Dokument entstand aus einer Zusammenarbeit des BSIs mit verschiedenen deutschen Herstellern von Heimroutern, Wirtschaftsvertretern, sowie mit Vertretern des OpenWrt Projektes und dem Chaos Computer Club. Diese trugen ihre Ideen und Vorstellungen zur Sicherheit von Routern zusammen und suchten Lösungen für Interessenkonflikte. Nach Veröffentlichung der Richtlinie im Jahre 2018 wurde diese allerdings unter Anderem von Vertretern des OpenWrt Projektes, sowie vom Chaos Computer Club (CCC), kritisiert. Nach Meinung dieser Interessengruppe sind die definierten Maßnahmen in der Technischen Richtlinie nicht ausreichend, um tatsächliche Angriffe auf Router zu verhindern.

* 1. **Bisherige Forschung**

Während der Einsatz von OpenWrt für spezialisierte Netzwerkumgebungen und zur Vereinheitlichung unterschiedlicher Netzwerkprotokolle beliebt zu sein scheint sind derzeit keine aktuellen Arbeiten zur Sicherheit von OpenWrt verfügbar. Ortega et al. veröffentlichte 2009 eine Arbeit über eine quelloffene Methode zum Verhindern von sogenannten ARP Poisoning Attacken. Sie nutzen in diesem Kontext OpenWrt lediglich als vielseitig unterstützte Testplattform [source]. Palazzi et al. nutzen den Funktionsumfang und die Anpassbarkeit der Firmware, um einen verbesserten Datendurchsatz in Heimnetzen mit verschiedenen W-Lan Geräten zu erreichen. Keine der derzeitigen Veröffentlichungen beschäftigt sich mit der Sicherheit von OpenWrt als Betriebssystem. Einzig Andrew McDonnell veröffentlichte in seinem Blog 2014 zwei Einträge über eine Sicherheitsanalyse von OpenWrt mittels des Tools checksec.sh[source] und entwarf eine verbesserte Version, in welcher bedeutend mehr Härtungsmaßnahmen aktiviert waren [source]. McDonnells Ergebnisse basierten jedoch auf Version 14.07 (Barrier Breaker) von OpenWrt, welche stark veraltet ist.   
 Die Forschung an Komponenten die OpenWrt ausmachen ist jedoch keinesfalls so eingeschränkt wie zuvor aufgezeigt. Der Linux Kernel, welcher einen grundlegenden Teil des OpenWrt Betriebssystems ausmacht, ist seit seiner Veröffentlichung 1991 ein andauerndes Gebiet der Forschung und Entwicklung, so auch in der IT-Sicherheit. Ebenso definiert sich OpenWrt über seine ca. 3800 zusätzlichen quelloffenen Pakete. Viele dieser Software-Erweiterungen existieren schon seit Jahrzehnten und ihre Integrität und Vertraulichkeit sind von den unzähligen Nutzern auf verschiedensten Plattformen anerkannt. Abschließend kann man feststellen, dass es zwar durchaus Forschung an Komponenten von OpenWrt gibt, jedoch OpenWrt selbst noch nicht oft mit Mittelpunkt der Forschung stand und die Sicherheitslage weitestgehend ungeklärt bleibt.

* 1. **Zielsetzung**

Ziel dieser Arbeit ist es die aktuelle Version von OpenWrt (19.7.04) anhand der BSI TR-03148 zu analysieren. Hierbei soll ein handelsüblicher, moderner Heimrouter, welcher vermehrt von OpenWrt Nutzern eingesetzt wird, genutzt werden. Es sollen die grundsätzlichen Sicherheitsmerkmale von OpenWrt mittels der technischen Richtlinie evaluiert werden. Ebenso soll die Anwendbarkeit der technischen Richtlinie auf quelloffene Netzwerk-Betriebssysteme ermessen werden. In einem weiteren Schritt werden die Ergebnisse der Untersuchung im Kontext anderer quelloffenen und proprietären Router-Betriebssysteme betrachtet. Darüber hinaus sollen statische Software Tests aller betrachteten Betriebssysteme als weitere Metrik dienen und einen differenzierteren Einblick in die Sicherheitslage gewähren. Abschließend muss sich kritisch mit den Ergebnissen, sowie der technischen Richtlinie, auseinandergesetzt werden. Die Ergebnisse der Arbeit können sowohl der Entwicklung von OpenWrt als auch unerfahrenen Endnutzern weitere Einblicke in die Sicherheit des Projektes liefern und somit langfristig die Resilienz der Heim- und SoHo Netzinfrastruktur stärken.

Kapitel 2

Grundlagen

2.1 Something

Kapitel 3

Methodik

3.1 Übersicht und Begründung der verwendeten Methodik

Die Methodik der Arbeit ist in großen Teilen durch die Technische Richtlinie vorgegeben. Auf eine genaue Durchführung wurde großer Wert gelegt. Die Testfälle wurden aufgrund ihrer Gruppierung in thematische Module in chronologischer Reihenfolge erarbeitet. Einzig solche Testfälle, welche spezifizierten, dass sie erst zum Ende der Testphase durchgeführt werden sollten, wurden nach Hinten gestellt. Da es in erster Linie um die Technische Richtlinie 03148 gehen soll, wurden weitere Tests, wie ein statischer Test mit dem Tool „FACT“[SOURCE], erst nach Vollendung der Richtlinie begonnen.   
 Die Testfälle der Technischen Richtlinie wurden, soweit möglich, mit den Programmen durchgeführt, welche in der TR selbst spezifiziert wurden. Die aufgeführte Software ist für die Überprüfung der Testanforderungen geeignet, sowie die Ergebnisse derselben seit vielen Jahren weitestgehend als korrekt akzeptiert. Hierzu zählt vor Allem das Programm nmap, welches aufgrund von verschiedenen Testrechnern in den Versionen 7.80, 7.90 und 7.91 verwendet wurde. Die Änderungshistorie von nmap gibt allerdings keinen Anlass zur Annahme, dass dies die Ergebnisse invalidiert [SOURCE]. Ebenso wurde airmon-ng / airodump-ng zum Prüfen verwendet. Diese Softwarepacket ist ebenfalls seit vielen Jahren angesehen. Zur Aufzeichnung von Netzwerkpaketen wurde Wireshark verwendet, welches neben der Kommandozeilenanwendung tcpdump häufig Verwendung findet. Im Rahmen der Tests wurde des Weiteren auf einige zweckspezifische Skripte in der Programmiersprache Python zurückgegriffen. Bei der Entwicklung wurde Wert auf einfache Ausführbarkeit, sowie eine geringe Zahl an externen Abhängigkeiten, gelegt, um eine wiederholbare Ausführbarkeit auch in der Zukunft zu gewährleisten.

3.2 Aufbau und Beschreibung der Testumgebung

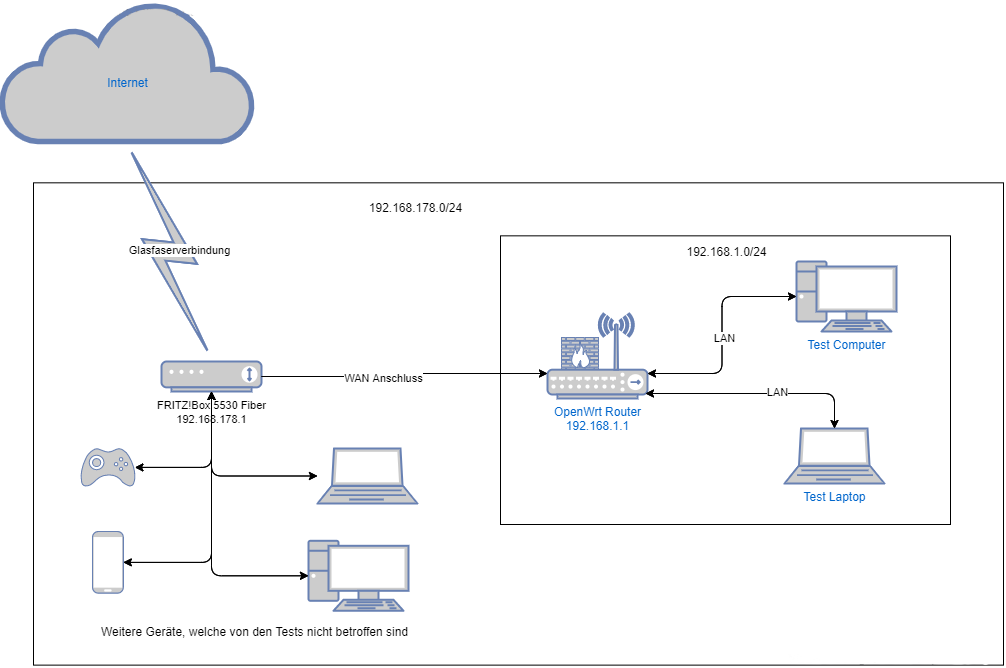
 Der genutzte Testaufbau soll einen reibungslosen Ablauf der Testfälle erlauben, sowie einfach reproduzierbar sein. Der Internetanschluss wurde durch den Internet Service Provider (ISP) bn:t Blatzheim Networks Telecom GmbH zur Verfügung gestellt. Der Glasfaseranschluss des ISP mündete in eine FRITZ!Box 5530 Fiber, welche das Subnetz 192.168.178.0/24 bereitstellt. Der WAN Port des mit OpenWrt 19.7.04 bespielten Heimrouters, ein TP-Link Archer C7 v.5, wurde mit dieser FRITZ!Box verbunden, sodass der OpenWrt fähige Router das Subnetz 192.168.1.0/24 aufspannen konnte. Ein Testcomputer wurde über LAN angeschlossen, ein weiterer Laptop per WLAN verbunden. Der Testcomputer wurde wahlweise mit Windows 10 Version 20H2 (Build 19042.685) oder Ubuntu 20.04 LTS betrieben. Auf dem Laptop kam Kali Linux zum Einsatz. Dieser Aufbau gibt dem Tester eine flexible Arbeitsumgebung, in welcher die Tests ungestört durchgeführt werden können. Durch die automatische Abtrennung des Netzes in das 192.168.1.0/24 Subnetz durch den OpenWrt Router sind Geräte des allgemeinen Heimnetzes von Portscans und Netzwerkpaketmitschnitten ausgeschlossen wodurch Tests performanter durchgeführt werden können, während andere Teilnehmer des Netzes ungestört weiterarbeiten können. Ebenso bietet der beschriebene Aufbau einfach die Möglichkeit weitere Netzteilnehmer oder Geräte hinzuzufügen. Die verwendeten Linux Distributionen, Ubuntu 20.4 LTS und Kali Linux, bieten dabei die notwendigen Programme und Möglichkeiten zur Durchführung der Testfälle.

Abbildung : Aufbau der Testumgebung mit Einteilung in Subnetze

2.3 Durchführung der Testfälle

2.3.1 Conformance Statement