**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?**

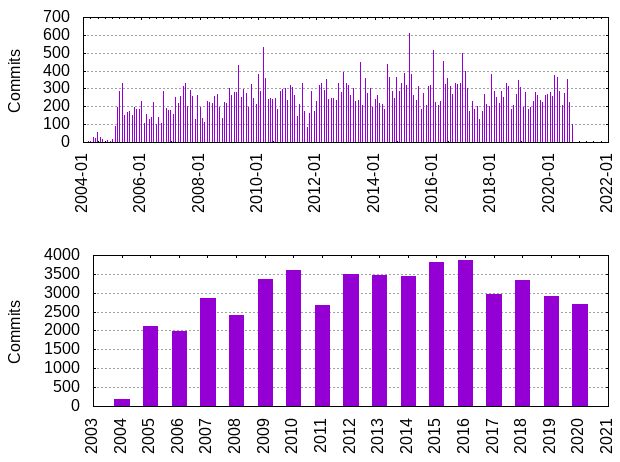
OpenWrt (**Open** **W**ireless **R**ou**T**er) ist ein quelloffenes Netzwerk-Betriebssystem für Router, welches auf GNU/Linux basiert und durch eine GNU General Public License (GPL) lizensiert ist. Die Installation umfasst einen bootloader, kernel, ein eigenes Dateisystem und ausgewählte Anwendungen. 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.   
 Die Entwicklung von OpenWrt begann 2004, nachdem der 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, welches eine Abspaltung von OpenWrt darstellte. 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 1: 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**

Privat

Unternehmen

Forschung / Entwicklung → von Website / ggf. Satura

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

TODO

* 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 sog. 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 Analyse von OpenWrt mittels des Tools checksec.sh[source] und ebenfalls 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.

* Forschung Linux Kernel
* Forschung Open Source allgemein
* Forschung Pakete – tested and trusted

* 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.