**Inhaltsverzeichnis**

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

# Abstract

# Zusammenfassung

Kapitel 1

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] wird 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].

* 1. Was ist OpenWrt?
  2. Relevanz und Verwendung von OpenWrt
  3. Beschreibung der TR-03148
  4. Bisherige Forschung
  5. Zielsetzung