Projektskizze

für das Fach Systemadministration

1. Einleitung – „Big brother is watching you“

1.1 Motivation

Im Rahmen der Aufdeckung des NSA-Skandals stellte sich heraus, dass Geheimdienste untereinander personenbezogene Daten und Informationen austauschen mit dem Ziel, Profile der Bürger zu erstellen um diese zu überwachen. Die brisanten Enthüllungen um Edward Snowden oder Wikileaks zeigten das Ausmaß im Zusammenhang mit Programmen wie PRISM(USA) und TEMPORA(GB) – um nur zwei Beispiele zu nennen. Daten werden dort auf Vorrat gespeichert, systematisch analysiert und vor allem für politische Zwecke ausgewertet. Dieser Umstand führt bei den Menschen zur sogenannten „Schere im Kopf“, da sie verunsichert sind was sie in der Öffentlichkeit noch sagen dürfen ohne in das Fadenkreuz der Geheimdienste zu gelangen. Das offizielle Statement „Krieg gegen den Terror“ zur Rechtfertigung von Überwachungsaktivitäten an allen Bürgern scheint langsam aber sicher in den Köpfen der Menschen zu bröckeln. Denn wer Böses tun will, wird dies im Normalfall nicht über WhatsApp oder Facebook kommunizieren.

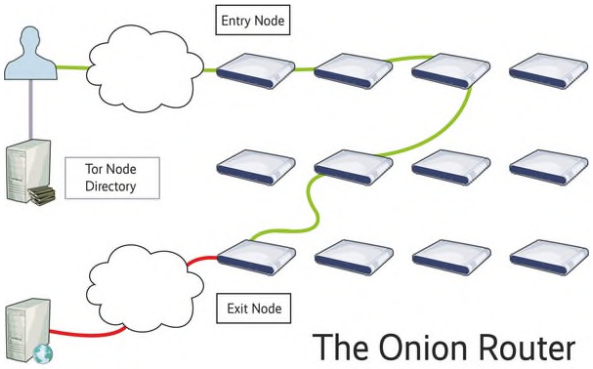
Momentan entwickeln wir uns Schritt für Schritt zu einer weltweiten Überwachungsgesellschaft. Wenn wir nicht anfangen unserer Verantwortung bewusst zu werden uns vor dieser Entwicklung zu schützen, wird es vielleicht schon bald möglich sein durch Big Data den „next step“ der Überwachung zu berechnen. Dieser Schritt könnte die vollautomatische Berechnung eines Gefahrenpotenzials politisch „Andersdenkender“ bedeuten oder z. B. durch das „Internet of Things“ zu einer Abschaltung bzw. Fremdansteuerung von Geräten des täglichen Gebrauchs. Nach einer reifen Überlegung der aufgedeckten „Skandale“ muss man sich die Frage stellen: Sind unsere Daten in den richtigen Händen?

Die Menschen müssen über alternative Verschlüsselungstechnologien, wie z.B. das Onion-Routing-Protocol, SSH oder VPN-Verfahren, aufgeklärt werden und in der digitalen Welt mehr Verantwortung übernehmen. Eine Möglichkeit sich etwas sicherer im Internet zu bewegen ist die sogenannte Tor Technologie.

1.2 Was ist Tor?

Tor (The Onion Router Project) ist ein Netzwerk, dass es einem Nutzer erlaubt sich anonymer im Internet zu bewegen. Nach einem Zufallsprinzip, führen verschiedene Router den Nutzer durch das innere des Tor-Netzwerks. Der Start ist immer ein Eingangsknoten, auch „Entry Node“ genannt, mit dem sich der Tor-Client verbindet. Diese Verbindung ist immer verschlüsselt und bietet daher einen klaren Vorteil gegenüber konventionellen Technologien. Innerhalb des Netzwerks wird die Source-IP-Adresse des Benutzers immer

durch den nachfolgenden Router überschrieben. Somit bleibt der Nutzer anonym, wenn das Datenpaket durch den Ausgangsknoten, auch „Exit Node“ genannt, in das Internet gelangt. Innerhalb des Netzwerks werden die Router zufällig ausgewählt um die Nachverfolgbarkeit zu verringern.



1.3 Raspberry-Pi als Tor-Router

Um dem Nutzer eine Möglichkeit zu bieten, mit einem eigenen Router über das Tor Netzwerk eine Verbindung aufzubauen ist es sinnvoll mit einer vergleichsweise günstigen Hardware zu arbeiten. Für solche Projekte bietet sich der Einplatinencomputer der britischen Firma Raspberry Pi Foundation an. Mit diesem Kleincomputer ist es möglich, individuelle Hard- und Software zu installieren um maßgeschneiderte Projekte kostengünstig durchzuführen. Außerdem sind Projekte mit dem Raspberry Pi trotz des geringen Preises gut dokumentiert, leistungsstark und durch die zugrundeliegende Architektur sehr flexibel für Entwickler.

2. Problemstellung – „Don't let the technology defeat you!“

Den meisten Nutzern die sich im Internet bewegen fehlen technische Grundkenntnisse um sich ausreichend vor der Massenspionage oder gar vor einzelnen Netzwerk-Angriffen zu schützen. Viele User nehmen sich erst gar nicht die Zeit um sich über solche Aktivitäten aufklären zu lassen, obwohl dies mit wenig Mühe auf verschieden Plattformen möglich wäre – auch ohne Fachwissen. Im Gegensatz dazu nutzen User gerne kostenlose Dienste wie Facebook, Snapchat oder Instagram und geben freiwillig Ihre Daten an die Öffentlichkeit – Nach dem Prinzip: „Ist doch eh kostenlos“. Die Realität zeigt aber, dass nichts umsonst ist – irgendwie bezahlt man immer.

Das Hauptproblem ist das zu große Vertrauen auf Softwaredienstleister oder kostenlosen Virenscannern. Dabei liefern die meisten kommerziellen Software-Lösungen kalkulierte Backdoors für Geheimdienste, die leider auch von Blackhat-Hackern dankend genutzt werden können.

Um diesem Problem zumindest ein wenig entgegenzuwirken soll im Fach Systemadministration ein Plug & Play Tor-Router mit W-LAN Access Point und zusätzlichem Fingerabdruckscanner zur Identifikation entwickelt werden. Außerdem soll ein zusätzliches „HowTo – Quick Start Guide“ verfasst werden um den Nutzer aufzuklären und eine Starthilfe zu geben.

3. Anforderungsanalyse

Der User benötigt ein Komplettsystem, ohne weitere Konfiguration oder umständliche Einrichtung, nach dem Plug & Play Prinzip. Es sollte möglich sein ohne Umwege eine „sichere“ und schnelle Verbindung zum Tor-Netzwerk aufzubauen. Da mobile Geräte statistisch gesehen am häufigsten benutzt werden, sollte eine Verbindung mit einem W-LAN Access Point ebenso gewährleistet sein wie ein Fingerabdrucksensor zur Authentifikation des zu verbindenden Users.

Internetnutzer sind nicht bereit viel Geld in Ihre virtuelle Sicherheit zu stecken, also sollte die bereitgestellte Lösung möglichst kostengünstig und leicht in Ihrer Bedienbarkeit sein. Außerdem sollte ein „Quick Start Guide“ beiliegen um dem User eine schnelle Möglichkeit zur Einführung und Verbindung zu ermöglichen.

4. Lösungsvorschläge

Um dem Endnutzer eine Lösung anzubieten werden nachfolgend zwei Lösungen gegenübergestellt und anschließend eines ausgewählt. Leider sind die Angebote solcher Dienste stark überschaubar, aber dennoch ratsam um zumindest sicherer und verantwortungsbewusster zu surfen. Die Probleme in Bezug auf Social-Media-Aktivitäten oder ein Restrisiko trotzdem ausgespäht zu werden bleiben bei beiden Lösungen weiterhin bestehen.

4.1 Tor-Browser über ein vollwertiges Betriebssystem

Funktion: Zugriff zum Tor-Netzwerk über einen stationären bzw. mobilen Computer mit vollwertigem Betriebssystem über das Tor-Browser-Package. Installation auf ein mobiles Endgerät wie z.B. Android ist nur sehr schwer und mit umfangreichen Knowhow möglich.
Kosten: Kostenloser Download
Mehrwehrt: Anonymeres Surfen mit bestehendem Computer.
Bewertung: Sowohl die Einrichtung, als auch die Handhabung dieser Variante ist trotz guter Anleitungen im Netz für einen Laien nicht ohne Starthilfe zu meistern. Außerdem fehlt hier insbesondere der Plug & Play-Gedanke, dass für die Zielgruppe unseres Projektes unabdingbar ist. Diese Möglichkeit der Verbindung zum Tor-Netzwerk wird in diesem Projekt nicht weiter erläutert.

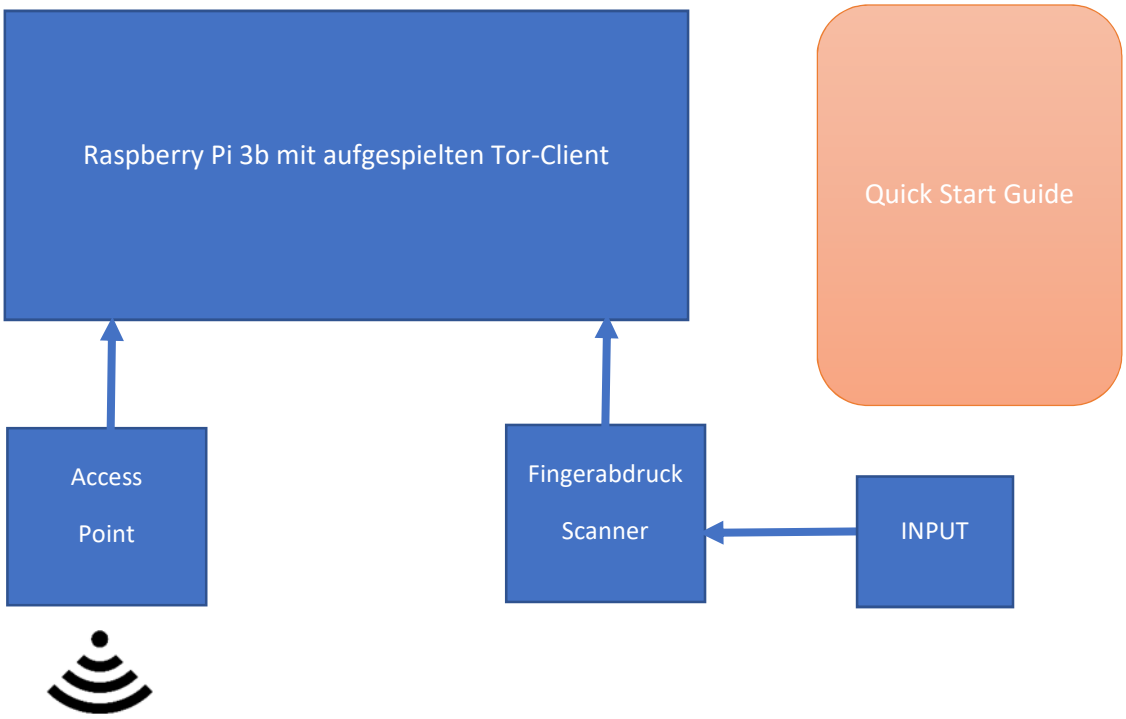
4.2 Entwicklung eines Raspberry Pi Tor Routers

Funktion: Der Benutzer kann sich mit dem Tor-Router in Form eines Raspberry Pi in das Tor-Netzwerk einloggen und anschließend anonymer surfen. Der große Vorteil ist die Nutzung von mobilen Endgeräten.
Kosten: Ca. 100 EUR für die Router-Hardware, Software kostenlos
Mehrwehrt: Unkompliziertes anonymeres Surfen auch mit mobilen Endgeräten.
Bewertung: Diese Variante ist für den Endnutzer stimmiger, da er ohne weiteres auf das Netzwerk kommt. Durch den Fingerabdruckscanner wird außerdem die Sicherheit des W-LAN Access Points erhöht. Dieses Projekt wird im Rahmen des Fachs Systemadministration ausgearbeitet und dokumentiert.

5. Ausgewählte Lösung

Im weiteren Projektverlauf soll die Lösung eines Raspberry Pi-Routers mit W-LAN Access Point und Fingerabdruckscanner zur Authentifikation des Benutzers entwickelt werden. Außerdem wird ein Quick Start Guide beigefügt. An dieser Stelle soll zur Lösung des Projektvorhabens nicht weiter eingegangen werden.

5.1 Komponentendarstellung



6. Fazit – „Fate, it seems, is not without a sense of irony“

Trotz der erhöhten Sicherheit durch das Tor-Netzwerk, im Vergleich zu konventionellen Technologien, sollte man möglichst darauf verzichten persönliche Daten im Internet preiszugeben. Um von der Anonymität der Tor-Technik zu profitieren, sollte man sich auch mit den richtigen Einstellungen zur Verbindung des Clients auseinandersetzen. Außerdem sollte immer darauf geachtet werden ein sicheres Passwort für alle Online-Aktivitäten zu wählen. Wichtig ist hier vor allem möglichst unterschiedliche Passwörter für verschiedene Online-Dienste zu nutzen. Wenn man auf Social-Media-Aktivitäten nicht verzichten kann, so sollte man zumindest darauf achten welche Informationen man in der digitalen Welt preisgibt. Zusammenfassend kann man sagen, dass die Verantwortung eines jeden Nutzers im Internet wichtiger ist als je zuvor.