Kryptoparty Whistleblowing

„Erstellen anonymer Identitäten (E-Mail Account) für das Internet ohne Preisgabe der IP Adresse“

Betreuer: Prof. Dr. Michael Anders
Bearbeiter: Louis Doneck (102811)

Hamburg, 14.07.2017

Inhaltsverzeichnis

Vorwort

Sollte man alles glauben, was in den Medien oder offiziellen Stellungnahmen von Behörden und Regierungen berichtet wird? Die Antwort ist natürlich jedem selber überlassen, allerdings sollte man diese Informationen mit Vorsicht genießen. Es ist schließlich nicht alles Gold, was auch glänzt. Und wären da nicht sehr mutige und verantwortungsbewusste Menschen, welche immer wieder auf Missstände hinweisen, würde Vieles erst gar nicht ans Licht der Welt kommen. Und so haben in der Vergangenheit immer wieder sogenannte Whistleblower für Aufregung aber auch für Aufklärung gesorgt.
Ohne diese Personen wäre unsere Welt ungerechter. Und gewisse Informationen, die für einige Menschen von großen Bedeutung sind, werden oftmals auch nur durch Whistleblowing bekannt gegeben.
Doch wer sind diese Menschen, welche teilweise persönliche und berufliche Risiken eingehen? Wie gehen Sie vor und durch welche Maßnahmen können sie sich schützen? Diese Seminararbeit wird im ersten Teil auf die Eigenschaften und historische Ereignisse des Whistleblowings eingehen. Der zweite Teil widmet sich verschiedenen Verfahren und Möglichkeiten, Anonymität im Internet und insbesondere beim Versenden von E-Mails zu bewahren. Abgerundet wird diese Arbeit mit einer Anleitung für das Erstellen anonymer Identitäten (E-Mail Accounts) für das Internet ohne Preisgabe der IP Adresse.

Whistleblowing

„Whistleblower sind Personen, die auf illegales Handeln, Missstände oder Gefahren für Mensch und Umwelt durch Veröffentlichung von meist geheimen Informationen hinweisen. Sie tun dies innerhalb ihres Betriebes, ihrer Dienststelle oder Organisation sowie auch extern gegenüber den zuständigen Behörden und der Presse.“
Diese zum Teil aus der Satzung des „Whistleblower-Netzwerk e.V.“ zitierte und zum Teil ergänzte Definition des Whistleblowings beschreibt in einem Satz, worum es bei diesem Thema geht.
Das Verschweigen oder Geheimhalten von relevanten Informationen, welche für die Öffentlichkeit oder einzelne Personen(gruppen) von Bedeutung sein könnten, findet viel zu häufig statt. Daher haben es sich einige Personen zur Aufgabe gemacht, dem entgegenzuwirken und entweder selber auf Missstände hinzuweisen oder aber Menschen bei ihren Vorhaben, dies umzusetzen, zu unterstützen.
Über den Ursprung des Wortes Whistleblowing lässt sich streiten. Es gibt verschiedene Vermutungen, wie es zu der Namensgebung kam. Als mögliche Herkunft des Begriffes gelten sowohl Polizisten, welche durch das Pfeifen auf ein Verbrechen aufmerksam machen wollten, als auch Schiedsrichter, die mit ihrer Pfeife Regelverstöße ahnden.

Historie

Doch zunächst lohnt sich ein Blick in die Vergangenheit. Erst Anfang der 70er Jahre entwickelte sich überhaupt der Begriff des Whistleblwoings, nachdem dieser erstmals in einem Artikel der New York Times („Hamilton: Blowing the Whistle on The Bossess“ im Jahr 1970 erwähnt wurde. Gefestigt hat sich der Begriff vor allem durch die 1971 von Ralph Nader organisierte „whistle blower’s conference“ in Washington D.C.[1]
Einer der bekanntesten Whistleblower aus der damaligen Zeit ist Daniel Elsberg, welcher Zugang zu den „Pentagon-Papieren“ hatte, diese (knapp 7000 Seiten Dokumente) über zwei Jahre lang kopierte und dann der New York Times und der Washington Post zuspielte. Die Veröffentlichung im Jahre 1971 legte dar, dass das Weiße Haus lange gewusst hatte, dass der Vietnamkrieg nicht zu gewinnen war und trotzdem den Kongress und das amerikanische Volk belogen hat.[2]

---

[1] http://www.whistleblower-net.de/whistleblowing/whistleblowing-im-
[2] http://www.spiegel.de/politik/ausland/pentagon-papers-washington-beichtet-letzte-vietnam-luegen-a-767493.html

Ein weiterer Skandal, welcher letztlich zum Fall des damaligen US-Präsidenten Richard Nixon führte, ist die Watergate Affäre. Eine der Hauptrollen hierbei spielte ein Whistleblower, auch unter dem Namen „Deepthroat“ bekannt, welcher anonym bleiben wollte. Er hat seine Informationen den beiden Reportern Bob Woodward und Carl Bernstein von der Washington Post anvertraut und erst im Alter von 91 Jahren seine wahre Identität der Öffentlichkeit Preis gegeben.[3]
Viele weitere mutige Personen oder Personengruppen haben in den folgenden Jahren dazu beigetragen, die Welt ein wenig fairer und transparenter zu machen. Heutzutage haben viele Menschen die Namen Edward Snowden, Chelsea Manning oder Julian Assange im Kopf. Aber auch anonyme Personen sind den Gang des Whistleblowers gegangen, wie beispielsweise bei den Panama Papers.

Arten und Phasen des Whistleblowings

Es gibt verschiedene Herangehensweisen, wie man am besten auf Missstände hinweisen kann. Diese sind abhängig vom der beruflichen und persönlichen Situation des Whistleblowers sowie dessen privaten und geografischen Umfeld. Generell kann man das Vorgehen aber in gewisse Phasen unterteilen, die fast jeder Whistleblower mehr oder weniger durchlebt.
So gibt es zwei Phasen (1 und 2) vor und zwei (4 und 5) nach dem tatsächlichen Whistleblowing (3).[4]

Die fünf Phasen des Whistleblowing

Es muss zunächst ein **Ereignis** (oder auch ein Unterlassen) eintreten, welches in der Wahrnehmung einer Person so gravierend unmoralisch, unfair oder schlicht illegal ist, dass diese sich dem nicht einfach entziehen möchte und daher weiter über das Ereignis nachdenkt.
In der anschließenden **Bewertung** der Situation spielen eine Vielzahl an Kriterien eine Rolle. Sowohl das private Umfeld, die Stellung in beispielsweise einer Organisation oder der Detailgrad der zugrunde liegenden Informationen

[3] http://www.sueddeutsche.de/politik/watergate-affaere-gestatten-deep-throat-1.842457
[4] http://www.whistleblower-net.de/whistleblowing/whistleblowing-im-detail/funf-phasen-des-whistleblowings/

als auch der Charakter der jeweiligen Person sind entscheidend. Das Ergebnis der Beurteilung des Ereignisses kann sehr verschieden ausfallen. Die Person kann sich unter folgenden Alternativen entscheiden: (1) Zufriedenheit und keine Notwendigkeit einer Handlung, (2) Notwendigkeit einer Handlung aber kein Handlungswille, (3) Flucht aus der Situation, (4) Einbeziehung Dritter oder (5) eigene Handlung zur Aufklärung oder Dämmung eines Missstandes. Vor allem Nummer 4 führt zu Whistleblowing. Nummer 5 in abgeschwächter Weise auch, allerdings kann hier die Handlung beispielsweise auch ein Weigern sein, sich an illegalen oder dubiosen Geschäften zu beteiligen.
In der Phase **Aktion** werden Dritte mit einbezogen, um die Bekämpfung des Missstandes zu erreichen. So werden oftmals geheime Informationen an Reporter und Journalisten weitergegeben. Hierbei ist festzuhalten, dass eben diese Reporter und Journalisten keine Whistleblower sind, sondern die ihnen zugetragenen Informationen nur öffentlich machen. Die Übertragung der Information kann sehr unterschiedlich ausfallen. Es kann persönlich oder über das Internet geschehen, anonym oder öffentlich und mit aber auch ohne Beweismaterial. Die Reporter haben nun die Aufgabe, die Informationen und Beweise gründlich zu prüfen und nach positivem Ausgang an die Öffentlichkeit zu gehen.
Anschließend können unterschiedliche **Reaktionen** festgestellt werden. Je nach Brisanz des Themas und Bekanntheit beziehungsweise Bedeutung von betroffenen Organisation oder Personen(gruppen) kann es einen riesigen medialen „Aufschrei“ geben oder die Sache verläuft im Sande. Die Reaktion kann Entlassungen und Neustrukturierungen zu Folge haben und im besten Fall auch ein ordentliches Aufarbeiten der Missstände.
Ob dies auch zur Zufriedenheit des Whistleblowers geschehen ist, wird durch die **Evaluation** klar. Je nachdem, ob Verbesserungen oder Änderungen vorgenommen wurden und wenn ja, in welchem Ausmaß, kann der Whistleblower sein Handeln als positiv und somit für abgeschlossen erachten oder aber die Phase Aktion wiederholen. So würde er in diesem Fall seine sensiblen Informationen an anderen Stellen platzieren und andere Dritte mit einbeziehen, von denen er sich mehr Unterstützung oder Aufmerksamkeit erhofft.

Grundsätzlich können zwei Arten von Whistleblowing nach dem Adressaten unterschieden werden, das **interne** sowie das **externe**. Beim internen befindet sich der Adressat innerhalb der Organisation, beim externen außerhalb. Beim internen werden beispielsweise über Hierarchiestufen hinweg Informationen preisgegeben, die zwar insgesamt noch in der Organisation verbleiben, aber trotzdem als kritisch angesehen werden können. Gerade wenn diese in die Hände von nicht vollständig der Organisationsleitung unterstehenden Organisationseinheiten wie Betriebs- oder Aufsichtsräten gelangen. Allerdings wird das externe Whistleblowing als

kritischer erachtet, da hiermit oftmals der Verlust der Kontrolle über die in der eigenen Organisation vorhandenen Informationen verbunden ist.[5]

Gefahren und Schutzmaßnahmen

Gerade wenn es kritische Informationen sind, die – aus Organisationssicht – in die falschen Hände geraten sind, müssen Whistleblower oftmals mit harten Konsequenzen rechnen. Abhängig von der Organisation und auch den Gesetzen im jeweiligen Land ist der Whistleblower mal mehr und mal weniger geschützt und somit teilweise einem traurigen Schicksal ausgesetzt.
So führt teilweise Mobbing sowie ungleiches und unfaires Behandeln der Whistleblower zu einem Grad der Unerträglichkeit. Häufig muss mit starken beruflichen Konsequenzen gerechnet werden und unter Umständen auch mit sehr langen Gefängnisstrafen sowie hohen Strafzahlungen. Im äußerst ungünstigen Fall kann es auch den Tod nach sich ziehen, wenn man beispielsweise eine gefährliche Gang verraten hat.

Whistleblowing ist mit Gefahren verbunden

In der vergangenen Jahren wurden die Gesetzte und Regeln (Compliance Officer häufiger in Unternehmen zu finden) in vielen Regierungen und Organisationen derart angepasst, dass sie tendenziell das Whistleblowing beziehungsweise den dadurch gefährdeten Whistleblower schützen. Es soll somit zur Verbesserung der allgemeinen Umstände kommen, sodass generell weniger Missstände aufgedeckt werden müssen. Sollte dies allerdings

[5] http://www.whistleblower-net.de/whistleblowing/whistleblowing-im-detail/formen/

trotzdem notwendig sein, sollen Gesetzte und Institutionen diejenigen Personen schützen, welche den Mut haben, diese Missstände anzusprechen.
Es gibt mittlerweile eine Vielzahl an Vereinen, welche Whistleblowing unterstützen und betroffene Personen beraten und deren Anonymität bewahren. So gibt es auch die seit Jahren bekannte Online Plattform Wikileaks, welche sich zum Ziel gesetzt hat, sensible aber für die Allgemeinheit wichtige Daten und Informationen zu veröffentlichen und den betroffenen Whistleblower zu schützen.
In den USA gibt es beispielweise den „Whistleblower Protection Act“, welches bundesstaatliche Mitarbeiter schützen soll. Ähnliche Gesetzte finden sich auch in anderen Ländern auf der ganzen Welt.
Um sich allerdings jegliche Unannehmlichkeiten und Gefahren vom Hals zu halten, bleibt nur der Weg der Anonymität, gerade wenn es um sehr brisante Themen geht. Und wie das, gerade in heutigen Zeiten, am besten realisiert werden kann, wird im folgenden Teil dieser Seminararbeit genauer unter die Lupe genommen.

Anonyme E-Mail Accounts

Natürlich können sensible Informationen direkt, also von Person zu Person, übermittelt werden, allerdings ist man dann weder anonym, noch ist diese Art der Übermittlung immer möglich. Gerade wenn Personen räumlich weit voneinander entfernt sind, ist die einzige Möglichkeit, in kurzer Zeit viele Informationen auszutauschen, das Internet. Und gerade um hier anonym zu bleiben müssen einige Dinge beachtet werden.

Anonymität im Netz

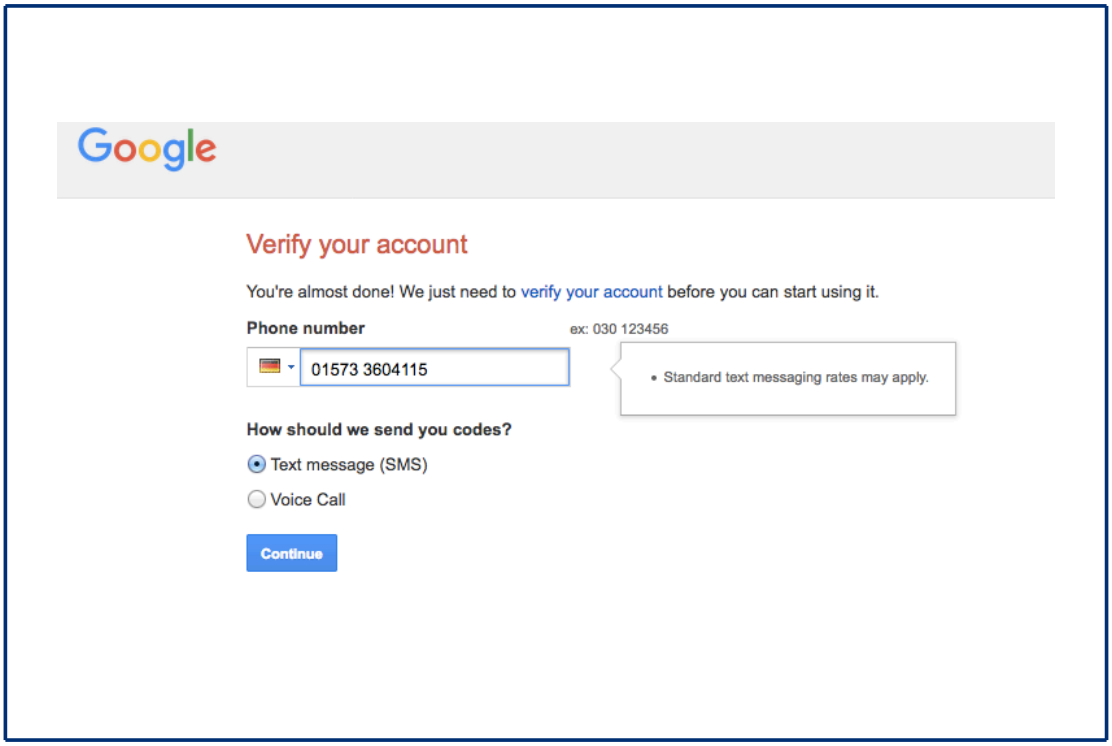
So gut wie jeder, der überhaupt für das Whistleblowing infrage kommen würde, hat Zugang zum Internet und nutzt dieses im Normalfall auch regelmäßig. Um nicht leicht von Geheimdiensten oder Sicherheitsfirmen aufgespürt werden zu können, müssen einige Voraussetzungen, was den Umgang mit dem Internet betrifft, geschaffen werden. So ist es fast schon unumgänglich, sich den Tor Browser herunterzuladen und anstelle der herkömmlichen Browser zu verwenden. Dadurch schützt man sich als Nutzer vor der Analyse seines Datenverkehrs, indem die eigene IP Adresse durch eine andere ersetzt wird. Es muss jedoch erwähnt werden, dass keine 100 prozentige Anonymität geboten werden kann, sollte es zu einer Überwachung einer ausreichend großen Anzahl von Tor-Knoten oder größeren Teilen des Internets kommen. Hierbei kann nahezu die komplette, über Tor abgewickelte Kommunikation nachvollzogen werden.[6]
Um noch einen Schritt weiter in Richtung Anonymität zu gehen, sollte die Linux-Distribution Tails (The Amnestic Incognito Live System) verwendet werden, um somit keine Spuren auf dem verwendeten Computer zu hinterlassen. Das System, welches insbesondere auf die Nutzung des Tor Netzwerkes setzt, kann beispielsweise über einen USB-Stick gebootet werden.[7]
Nun ist man vorbereitet und kann trotz des Surfens im Internet seine Privatsphäre schützen.

Unteschied herkömmlicher vs. anonymer E-Mail Accounts

Um nun aber sensible Daten einer bestimmten Person oder Organisation zukommen lassen zu können, ohne diese dabei persönlich treffen oder einen Brief in deren Briefkasten stecken zu können, müssen andere Methoden

[6] https://svn.torproject.org/svn/projects/design-paper/tor-design.html
[7] https://tails.boum.org/about/index.de.html

hinhalten. Daher bietet sich das Versenden von E-Mails an. Allerdings fliegt die Anonymität hier ziemlich schnell und bereits während des Anmeldeprozesses auf, sollte man es bei den herkömmlichen E-Mail Providern wie GMX oder Gmail probieren. So müssen teilweise bereits vorhandene E-Mail Adressen angegeben werden oder es wird (wie im nächsten Bild zu erkennen), nach der Handynummer gefragt, um einen Registrierungscode zu erhalten. Außerdem geben diese Anbieter häufig ohne größeres Zögern Daten an Dritte (andere Unternehmen oder Regierungen) weiter.



Abfragen der Handynummer bei der Gmail Registrierung

Daher muss man sich nach Alternativen umsehen, sollte man das Whistleblowing über den Inhalt einer E-Mail praktizieren. Man kann (über das Tor Netzwerk) beispielsweise Dokumente bei Wikileaks hochladen. Aber wenn Informationen an eine bestimmte Person gelangen sollen, kann dies am besten über E-Mails geschehen. Um hier trotzdem die Anonymität zu bewahren, kann man sich verschiede Anbieter zu nutze machen und so sicher und anonym kommunizieren.
Mögliche E-Mail Provider, welche absolute Anonymität und weitere Vorzüge versprechen sind unter anderem folgende: guerrillamail.com, yandex mail, hushmail, anonymouse, sendanonymousemail, mailinator und anonymousspeech. Einige dieser Provider bieten auch sogenannte Burner Accounts an, mit denen sich entweder nur Mails verschicken oder empfangen lassen, und dies auch meistens nur für einen kuren Zeitraum. Dies bietet sich vor allem an, um Spam zu entgehen.

Nach Testen einiger der eben genannten Provider hat sich vor allem einer herauskristallisiert. So bietet die Seite www.anonymousspeech.com eine webbasierte E-Mail Plattform, welche einen 14-tägigen, kostenlosen Testaccount ermöglicht. Denn das ist der Haken an der Sache, da die meisten Provider eine einmalige oder sich wiederholende Zahlung verlangen. Auch bei anonymousspeech kann man mit dem Testaccount nur auf bestimmt Funktionen zugreifen, allerdings sollten diese für das Whistleblowing reichen, wenn man nicht riesige Dateien versenden möchte. Denn um Anhänge zu verschicken, muss sich der Account einem kostenpflichtigen Upgrade unterziehen.
Anonymousspeech bietet jedoch auch einige Features und Sicherheitsvorkehrungen, die diesen Provider äußerst interessant für den anonymen E-Mail Verkehr machen.[8]

Security Facts	Features
- Anonyme IP - 128-bit SSL encryption - Keine Log Dateien - Kontanter Umzug der Server - Encrypted Login und Passwort - Löschen der Accounts - PGP Secure E-Mail - Anti Phishing Schutz (sign-in seal)	- Lesebenachrichtigung - Sichere Datei Ablage - Anonymes Datensharing (optional Selbstzerstörung) - Zeitverzögerte E-Mail - Anhänge bis 15MB

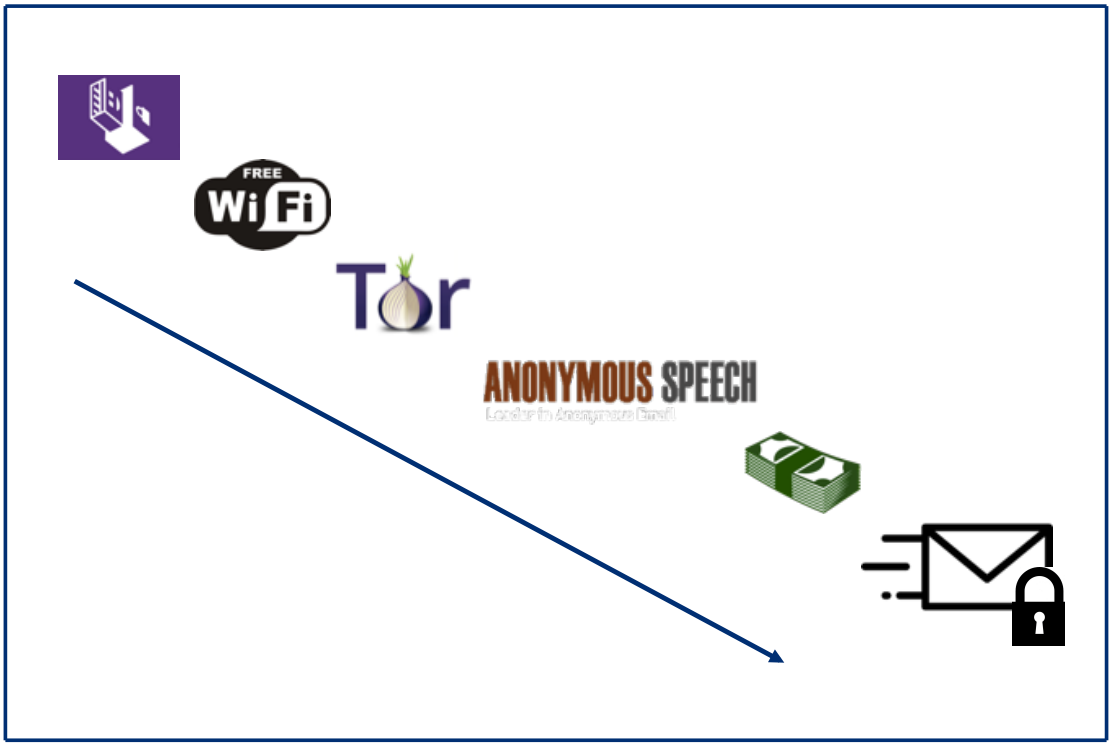
Security Facts und Features von anonymousspeech

So wird nach keiner Telefonnummer oder bereits bestehenden E-Mail Adresse gefragt. Man kann sich unkompliziert und nur mit Benutzernamen und Passwort registrieren. Zudem bieten der Anti Phishing Schutz sowie 128-bit SSL encryption und encrypted Login und Passwort weitere Vorteile. Zusätzlich behauptet anonymousspeech, dass ihre Server konstant unter Bewegung sind (beispielsweise Malaysia, Japan und Panama) und sich immer außerhalb der EU und den USA befinden. Die Länder, in denen die Server stehen, haben entweder keine Gesetzte bezüglich anonymer E-Mails/Kommunikation oder aber ausdrücklich die Privatsphäre schützende Gesetze.

[8] https://www.anonymousspeech.com/

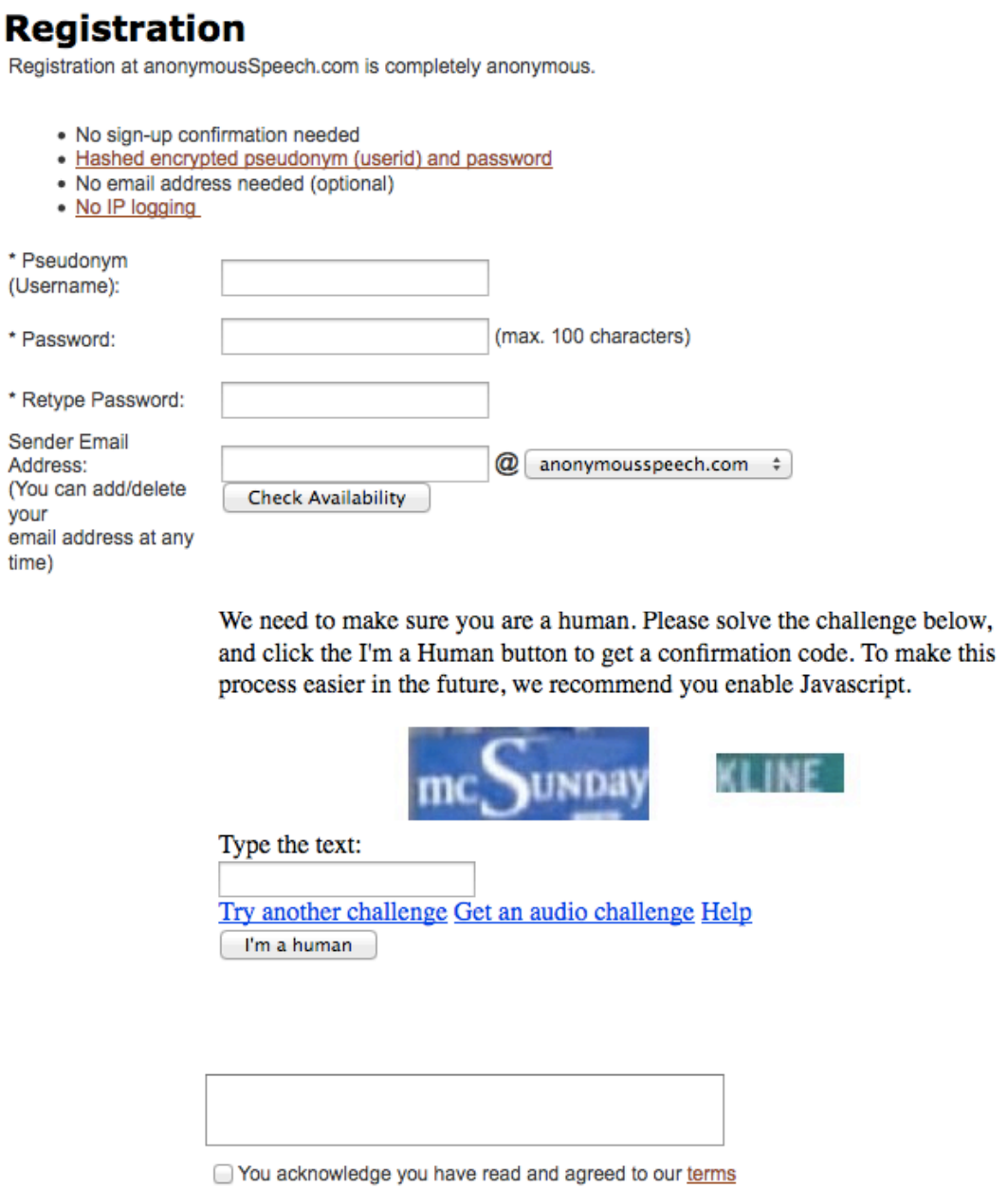
E-Mail Whistleblowing Tutorial

Doch wie geht man nun konkret vor, wenn einem sensible Informationen digital zur Verfügung stehen und per Mail an einen Adressaten des Vertrauens versendet werden sollen? Folgende Grafik visualisiert den optimalen Vorgang des Whistleblowings, wenn man über dies über anonymousspeech machen möchte. Im folgenden werden die einzelnen Schritte genauer beschrieben.



Vorgehensweise zur Erhaltung der Anonymität beim Whistleblowing

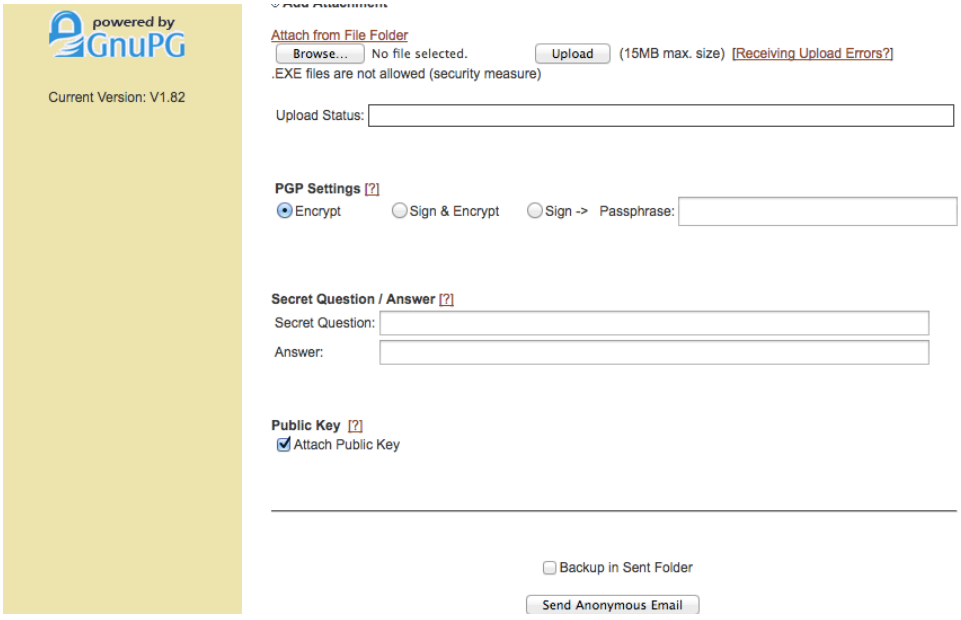
Wie bereits erwähnt, sollte man zunächst über Tails in das Tor Netzwerk gehen (somit auch die MAC Adresse gespooft), um hierüber die verschiedensten gewünschten Internetseiten aufzurufen. Am besten auch nicht im eigenen WLAN bei sich zuhause sondern in einem öffentlichen, frei zugänglichen Wifi, da hier überhaupt nicht auffällt, dass dieses Netz vom Whistleblower benutzt wird. Nun kann man sich bei anonymousspeech registrieren (siehe folgende Grafik). Wichtig ist nur, dass man sich sowohl sein Pseudonym als auch das Passwort merkt und den Nutzungsbedingungen zustimmt. Um anonymousspeech vollumfänglich nutzen zu können, muss allerdings das Java Skript im Tor Netzwerk ermöglicht werden.



Registrierungsseite bei anonymousspeech

Nach der Registrierung kann entweder sofort eine Mail verschickt werden, wenn man keinen Anhang (bis zu 15 MB möglich) hinzufügen möchte. Sollte dies allerdings notwendig sein, muss der Account ein Upgrade bekommen, welches kostenpflichtig ist. Hier bietet anonymousspeech verschiedene Bezahlmethoden an, welche die Anonymotät teilweise sofort aufheben. Da die Bezahlung per Kreditkarte hierfür sehr ungünstig ist, bieten sich noch Bitcoins oder Barzahlung an. Wenn man noch keine Bitcoins besitzt und sich den Erwerb auch nicht zutraut, kann man immer noch Bar bezahlen. Per Post soll dann ein gewisser Betrag (je nach Laufzeit des Upgrades) in einer von verschiedenen vorgegebenen Währungen (auch nur mit Scheinen) an einen M.Weber in der Schweiz geschickt werden. Sobald das Geld eingetroffen ist

(die Adresse ist auf der Internetseite zu sehen) kann der Account auf etliche Features zugreifen und auch Anhänge verschicken.
Um sich nun noch weiter abzusichern kann man die Mails auch verschlüsseln. Anonymousspeech bietet bereits im Webbrowser integriert eine PGP Secure Mail an.[9] Hier kann hat man allerdings nicht selber in der Hand, ob und wie wirklich verschlüsselt wird. Um zu verbergen, womit und ob überhaupt verschlüsselt wurde, bietet sich Academic Signature im "NADA-CAP-Modus" an. Generell kann man nicht wirklich wissen, wie die Mails gehandhabt werden und ob es wirklich so anonym zugeht, wie versprochen. So oder so, da man über Tails im Tor Netzwerk aktiv ist, ist zumindest die eigene IP Adresse verborgen. Wenn man sich nun aber für die Verschlüsselung über den Browser entscheiden sollte, muss zunächst ein PGP Keypair erstellt werden. Dazu muss man sich eine Passphrase ausdenken. Um nun auch E-Mails verschlüsselt zu verschicken, wird noch der Public Key des Adressaten benötigt und unter „Import Public Key“ importiert. Nun kann auch schon die Mail verschickt werden (mit eigenem Public Key als Anhang) und sowohl verschlüsselt als auch digital unterschrieben werden, wie auf folgender Abbildung zu sehen.



PGP Secure Mail by anonymousspeech

Durch die eben genannten Schritte ist ein relativ simpler Ablauf gesichert, der es einem potentiellen (nicht extrem IT-affinen) Whistleblower ermöglich, anonym zu bleiben und trotzdem seine sensiblen Informationen an den gewünschten Adressaten weiterzugeben. Auch einem weiteren E-Mail Austausch zwischen Whistleblower und Adressat steht nichts mehr im Wege.

[9] https://anonymousspeech.com/secure_email_write.aspx

Fazit

Die Möglichkeiten, heutzutage zu kommunizieren sind fast grenzenlos. Allerdings ist die Privatsphäre dabei äußerst selten geschützt. Daher haben sich Menschen die Mühe gemacht, Software und Systeme zu entwickeln, welche eine gewisse Anonymität gewähren.
Um auf Missstände in Organisationen oder Regierungen hinzuweisen, gehört eine gehörige Portion Mut dazu. Vor allem, wenn man sich dadurch oder auch danach der Öffentlichkeit beziehungsweise der Organisation oder Behörde stellt. In manchen Fällen wäre ganz klar, wer bestimmte Informationen „geleaked“ hat und daher wäre auch die Anonymität nicht gegeben. Ist dies jedoch nicht klar, so sollte diesen pflichtbewussten Menschen die Möglichkeit geboten werden, ihre Privatsphäre schützen und anonym bleiben zu können. Wie dies gelingen kann, wurde in dieser Seminararbeit erläutert und kann somit als Anleitung für das Whistleblowing via E-Mail Accounts dienen, ohne dabei die eigene IP Adresse preisgeben zu müssen.

Literaturverzeichnis

http://www.whistleblower-net.de/whistleblowing/whistleblowing-im-detail/begrifflices/

http://www.spiegel.de/politik/ausland/pentagon-papers-washington-beichtet-letzte-vietnam-luegen-a-767493.html

http://www.sueddeutsche.de/politik/watergate-affaere-gestatten-deep-throat-1.842457

http://www.whistleblower-net.de/whistleblowing/whistleblowing-im-detail/funf-phasen-des-whistleblowings/

http://www.whistleblower-net.de/whistleblowing/whistleblowing-im-detail/formen/

https://svn.torproject.org/svn/projects/design-paper/tor-design.html

https://tails.boum.org/about/index.de.html

https://www.anonymousspeech.com/

https://anonymousspeech.com/secure_email_write.aspx