

**Brixen, der 2. Mai 2017**



**Fachrichtung Informatik:**

 **Sicherheit im Netz**

**Erstellt von Tobias Oberhauser**

**Betreut von Ulrich Rainer**

**Inhaltsverzeichnis:**

1. [Einleitung 3](#_Toc480888772)

[1.1 Warum Verschlüsselung? Ich habe doch gar nichts zu verbergen! Oder? 3](#_Toc480888773)

[1.2 Sind meine vertraulichen Informationen auf Google sicher? 3](#_Toc480888774)

[1.3 Wie kann man sich schützen? 3](#_Toc480888775)

1. [Hauptteil 3](#_Toc480888776)

[2.1 Google Konto 3](#_Toc480888777)

[**2.1.1** **Zwei-Stufen-Verifizierung** 3](#_Toc480888778)

[**2.1.2** **Sicherheitsphilosophie von Google:** 4](#_Toc480888779)

[2.2 Gmail 4](#_Toc480888780)

[**2.2.1** **Wie sieht es hier mit der Sicherheit aus?** 4](#_Toc480888781)

[**2.2.2** **Mögliche Erweiterung: PGP (Pretty Good Privacy)** 4](#_Toc480888782)

1. [Schluss 5](#_Toc480888783)

# **Einleitung**

## ****Warum Verschlüsselung? Ich habe doch gar nichts zu verbergen! Oder?****

Es geht nicht darum, ob man etwas zu verbergen hat, aber manche Dinge möchte man lieber vertraulich behandeln. Wenn Sie z.B. geschäftliche Nachrichten lieber im verschlossenen Umschlag statt als Postkarte verschicken, dann sollte es für Sie selbstverständlich sein, Ihre elektronische Post zu verschlüsseln. [1]

Durch die Abhörskandale rückt die Sicherheit der täglichen Kommunikation in das öffentliche Interesse. Immer häufiger treten Lücken zutage, über die Angreifer den Datenverkehr mitlauschen können. Die Folgen für Unternehmen reichen von Betriebsspionage über Diebstahl von wichtigen Firmen- und Kundendaten und Sabotage bis hin zur Erpressungsfällen. [2]

Als Anbieter von Software und Services ist es Google wichtig, die Daten-Sicherheit zu gewährleisten, um das Vertrauen der Community zu festigen. Die Produkte sollen alle Anforderungen erfüllen ohne Sicherheitslücken aufzuweisen. Mittels Updates, Erweiterungen und Support sollen die Risiken minimiert werden. Grundlage für eine positive Entwicklung der Produkte ist eine gute Interaktion mit den Usern.

In dieser Arbeit werden die Risiken der Benutzung von Google Dienste aufgezeigt, mögliche Risiken veranschaulicht und Lösungen vorgeschlagen.

# **Hauptteil**

## ****Google Browser****

Sensible Daten sind in Google Chrome nicht sicher, da Kreditkartennummern, Telefonnummern, Kontodaten und ganze E-Mails als Klartext, also als unverschlüsselter Text, im Browser-Cache abgespeichert werden. Browser-Cache ist ein [Puffer-Speicher](https://de.wikipedia.org/wiki/Cache) des [Webbrowsers](https://de.wikipedia.org/wiki/Webbrowser), in dem bereits abgerufene Ressourcen lokal auf dem Rechner des Benutzers als Kopie aufbewahrt werden. [3] Wird eine Ressource später erneut benötigt, ist sie aus dem Cache schneller abrufbar, als wenn sie erneut heruntergeladen werden müsste. Die Firma Identity Finder, weist darauf hin, dass kein physischer Zugriff auf den [Rechner](http://partners.webmasterplan.com/click.asp?ref=119198&site=9853&type=text&tnb=29&subid=yield&diurl=http%3A%2F%2Fwww.saturn.de%2F%3Frbtc%3Daff%7Ccon%7C%24ref%24%7C%7C%7C%7C) nötig ist, um gespeicherte Informationen mitzulesen. Suchprogramme und Schadsoftware, die auf dem Rechner eingeschleust werden, scannen Dateitypen auf Klartext-Informationen. Einmal gespeichert, bleiben die persönlichen Daten als Klartext im Cache. Die Option, den Browser-Cache nach jeder Sitzung automatisch zu leeren, bietet Chrome leider nicht an. Da Chrome den Browser-Cache nicht automatisch nach jeder Sitzung leert, ist es sinnvoll auf ein Browser-Plug-in zurückzugreifen: Click&Clean für Google Chrome bietet zahlreiche Möglichkeiten, die Browser-Sicherheit zu erhöhen. [4]

## ****Google Konto****

### **Zwei-Stufen-Verifizierung**

Google Konten unterstützen die [Zwei-Stufen-Authentifizierung](https://de.wikipedia.org/wiki/Zwei-Faktor-Authentifizierung). Nach der Anmeldung auf einem neuen Gerät müssen Benutzer ihre Identität durch eine zweite Methode nachweisen. Normalerweise ist diese zweite Methode ein sechsstelliger Code, der mit der [Google-Authenticator](https://de.wikipedia.org/wiki/Google_Authenticator)-App generiert wurde. Alternativ kann der Code per SMS oder Anruf abgerufen werden.

Als Sicherheitsupdate kündigte Google 2014 die Integration von [Universal Second Factor (U2F)](https://de.wikipedia.org/wiki/U2F) in den Chrome-Browser an. Benutzer können den U2F-Sicherheitscode als Primärmethode der Zwei-Stufen-Verifizierung festlegen, um unabhängig von Verifizierungscodes zu sein, die per SMS gesendet oder in ihren Mobilgeräten erzeugt werden. Im Vergleich zu sechsstelligen Codes bietet der U2F-Sicherheitscode besseren Schutz vor Phishing. Unter Phishing versteht man Versuche über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

Wenn sich ein Nutzer anmeldet, bei dem Google den Verdacht hat, dass er Opfer von Angriffen wurde, wird ein Warnhinweis angezeigt und bei Bedarf weitere Maßnahmen eingeleitet. [5]

## ****Gmail****

Gmail protokolliert die letzten 10 Zugriffe auf das Postfach mit IP-Adresse und Zeitstempel. Zudem zeigt Gmail an, wo dasselbe Postfach außerdem geöffnet ist (IP-Adresse und Browsertyp). Zusätzlich verfügt der [Spamfilter](https://de.wikipedia.org/wiki/Spamfilter) von Gmail über ein Community-System: Sobald ein Benutzer eine E-Mail als Spam markiert, dient diese Information zur Erkennung von ähnlichen Nachrichten. Seit 2015 versucht Google künstliche [neuronale Netze](https://de.wikipedia.org/wiki/Neuronales_Netz) einzusetzen um Spam zu erkennen. Künstliche neuronale Netze stellen einen Zweig der [künstlichen Intelligenz](https://de.wikipedia.org/wiki/K%C3%BCnstliche_Intelligenz) dar.

Als Sicherheitsmaßnahme gegen [Viren](https://de.wikipedia.org/wiki/Computervirus) werden E-Mails, mit ausführbaren Dateien als Anhang, nicht zugestellt. Wenn etwas entdeckt wird, das Google als „Unregelmäßigkeit, die auf einen Missbrauch hinweist“ bezeichnet, kann das Konto automatisch gesperrt werden. Die Sperre dauert 1 Minute bis 24 Stunden, je nach Art der entdeckten Aktivität.

E-Mails können auf dem Weg durchs Internet von Rechnern gelesen und auch verändert werden, ohne dass es der Empfänger merkt. Experten gehen davon aus, dass heute ein Großteil des Datenverkehrs automatisiert überwacht und ausgewertet wird.

### **Mögliche Erweiterung: PGP (Pretty Good Privacy)**

Die Verschlüsselung der Nachrichten, dass nur der tatsächliche Empfänger sie lesen kann. Es werden Verschlüsselungsalgorithmen benützt, an denen sich selbst Geheimdienst die Zähne ausbeißen. Deshalb versuchten die USA den Export von PGP um jeden Preis zu verhindern, allerdings nicht erfolgreich.

Herkömmliche Verfahren verwenden für das Codieren und Decodieren denselben Schlüssel (symmetrischen Verfahren). Dafür müssen Absender und Empfänger sich auf einen Schlüssel einigen und diesen austauschen. Wenn der Angreifer den Schlüssel kennt, kann er alle weiteren Nachrichten mitlesen.

Im Gegensatz zu diesem symmetrischen Verfahren verwendet PGP eine asymmetrische Verschlüsselung. Dabei besitzt jeder Kommunkationspartner zwei Schlüssel: Einen privaten und einen öffentlichen Key. Den öffentlichen Schlüssel kann man beliebig verteilen. Mit dem öffentlichen Schlüssel kann man Nachrichten nur verschlüsseln, aber nicht lesen. Nur der Besitzer kann die Nachricht mit seinem privaten Schlüssel entziffern.

Man kann mit PGP eine Nachricht signieren oder auch verschlüsseln. Die Signatur dient dazu, die Echtheit der Nachricht zu garantieren, also dass sie vom behaupteten Absender ist ([Authentizität](https://de.wikipedia.org/wiki/Authentizit%C3%A4t#Informatik)) und nach der Signierung nicht verändert wurde ([Integrität](https://de.wikipedia.org/wiki/Integrit%C3%A4t_(Informationssicherheit))).

Ein möglicher Angriff ergibt sich aus dem Vorgehen, Nachrichten zuerst zu signieren und dann zu verschlüsseln. Der Empfänger kann die signierte Nachricht nach dem Entschlüsseln mit gefälschtem Absender an eine dritte Person weiterleiten. Falls der Adressat in der Nachricht nicht namentlich genannt ist, kann die gültige Signatur den Eindruck erwecken, sie sei direkt vom ursprünglichen Sender an diese dritte Person geschickt worden. Daneben wurde kritisiert, dass die Public Keys auf Servern liegen, auf die jeder Lese- und Schreibzugang hat. Dort wurden falsche Schlüssel abgelegt.

# **Schluss**

# **Quellen:**

[1] <https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/wozu.htm> (02.05.17)

[2] <https://www.giepa.de/datensicherheit-auch-beim-e-mail-verkehr> (02.05.17)

[3] <https://de.wikipedia.org/wiki/Browser-Cache> (02.05.17)

[4] <http://www.inkognito.it/wp2/?p=2008> (02.05.17)

[5] <https://de.wikipedia.org/wiki/Google-Konto#Sicherheit> (02.05.17)

1. <https://de.wikipedia.org/wiki/Gmail#Sicherheit> (02.05.17)
2. <https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/wasdas.htm>
3. [https://de.wikipedia.org/wiki/Pretty Good Privacy](https://de.wikipedia.org/wiki/Pretty%20Good%20Privacy)

<https://www.datenschutzbeauftragter-info.de/wp-content/uploads/2014/04/it-sicherheit-51.jpg> (02.05.17)

<https://i.ytimg.com/vi/YGym1Y0y9j4/hqdefault.jpg> (01.04.17)