



**Sicherheit im Netz**



**von Tobias Oberhauser**

**Inhaltsverzeichnis:**

1. Warum Verschlüsselung? Ich habe doch gar nichts zu verbergen! Oder? 2

1.1 Sind meine vertraulichen Informationen auf Google sicher? 2

1.2 Wie kann man sich schützen? 2

1. Google Konto 3

2.1 Zwei-Stufen-Verifizierung 3

2.2 Sicherheitsphilosophie von Google 3

1. Gmail 3
   1. Wie sieht es mit der Sicherheit aus? 3
   2. Mögliche Erweiterung: PGP 4
2. **Warum Verschlüsselung? Ich habe doch gar nichts zu verbergen! Oder?**

Es geht gar nicht so sehr darum, ob man etwas "zu verbergen" hat. Aber manche Dinge möchte man lieber vertraulich behandeln. Wenn Sie persönliche oder geschäftliche Nachrichten lieber im verschlossenen Umschlag statt als Postkarte verschicken, dann sollte es für Sie selbstverständlich sein, auch Ihre elektronische Post zu verschließen.

* 1. **Sind meine vertraulichen Informationen auf Google sicher?**

Nein, nicht zu 100%. Google Chrome speichert sensible Informationen wie Kreditkarten- und Versicherungsnummern, Telefonnummern, Kontodaten, E-Mail-Adressen und ganze E-Mails als Klartext im Browser-Cache.

Die Firma Identity Finder, weist darauf hin, dass kein physischer Zugriff auf einen [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 derart gespeicherte Informationen auszulesen. Diverse Such-Programme würden jeden Dateityp auf Klartext-Informationen scannen. In Verbindung mit entsprechender Schadsoftware, die auf einem Rechner eingeschleust werde, sei es kein Problem, die Informationen zu bekommen.

Das Problem: Einmal gespeichert, bleiben die persönlichen Daten unverschlüsselt im Cache. Die Option, den Browser-Cache nach jeder Sitzung automatisch zu leeren, bietet Chrome nicht an. Es braucht also nicht unbedingt Malware, um an die Daten zu kommen. Wer seinen Rechner beispielsweise zur Reparatur bringt, ihn verkauft oder Dritten überlässt, geht das Risiko ein, dass sein Browser-Cache ausgelesen wird.

* 1. **Wie kann man sich schützen?**

Löschen Sie den Cache, die AutoFill-Formulardaten und den Browserverlauf regelmäßig per Hand. Noch praktischer wäre es, wenn das automatisch passieren würde. Da Chrome diese wichtige Option nicht anbietet, müssen Sie auf ein Browser-Plug-in zurückgreifen: [Click&Clean](http://www.chip.de/downloads/Click-Clean-fuer-Google-Chrome_42414706.html) für Google Chrome bietet zahlreiche Möglichkeiten, die Browser-Sicherheit zu erhöhen.

1. **Google Konto**
   1. **Zwei-Stufen-Verifizierung**

Ein Google-Konto unterstützt die eine Form der [Zwei-Faktor-Authentifizierung](https://de.wikipedia.org/wiki/Zwei-Faktor-Authentifizierung). Nach der Aktivierung müssen Benutzer ihre Identität nach der Eingabe ihres [Benutzernamens](https://de.wikipedia.org/wiki/Benutzername) und Passworts durch eine zweite Methode nachweisen, wenn sie sich an einem neuen Gerät anmelden. Normalerweise geben sie dazu einen sechsstelligen Code ein, der mit der [Google-Authenticator](https://de.wikipedia.org/wiki/Google_Authenticator)-App generiert wurde. Die App funktioniert auch ohne Internet. Alternativ können Codes per SMS/Anruf an das Mobilgerät gesendet werden.

2014 kündigte Google die Integration von [Universal Second Factor (U2F)](https://de.wikipedia.org/wiki/U2F) in den Chrome-Browser an, wodurch der Einsatz eines physikalischen Sicherheitscodes für die Zwei-Stufen-Verifizierung ermöglicht wurde. 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 und macht ein Mobilgerät bei der Anmeldung überflüssig.

Wenn sich ein Nutzer anmeldet, bei dem Google den Verdacht hat, dass er Opfer von staatlichen [Phishing](https://de.wikipedia.org/wiki/Phishing)- oder [Malware](https://de.wikipedia.org/wiki/Schadprogramm)-Angriffen wurde, wird ein Warnhinweis angezeigt.

* 1. **Sicherheitsphilosophie von Google:**

Als Anbieter von Software und vielen Services ist es wichtig, die Daten-Sicherheit zu gewährleisten, um das Vertrauen der Community nicht zu verlieren. Trotzdem sollen die Produkte alle Anforderungen erfüllen ohne Sicherheitslücken zu bieten. Mittels Updates, möglichen Erweiterungen und diversen Internet Foren sollen die Risiken im Netz möglichst minimiert werden. Google erhofft sich auch eine gute Zusammenarbeit mit ihren Usern, deshalb können User entdeckte Sicherheitslücken melden.

1. **Gmail**
   1. **Wie sieht es mit der Sicherheit aus?**

Gmail protokolliert die letzten 10 Zugriffe auf das Postfach (IP-Adresse und Zeitstempel). Zudem zeigt es an, wo dasselbe Postfach außerdem geöffnet ist (IP-Adresse und Browsertyp). Der [Spamfilter](https://de.wikipedia.org/wiki/Spamfilter) von Gmail verfügt über ein Community-System: Sobald ein Benutzer eine E-Mail als Spam markiert, dient diese Information dem System als Hilfe zur Identifizierung künftiger ähnlicher Nachrichten an alle Gmail-Benutzer. Seit 2015 benutzt Google künstliche [neuronale Netze](https://de.wikipedia.org/wiki/Neuronales_Netz) um Spam zu erkennen.

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

E-Mails können leider von vielen Rechnern 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 nach Schlüsselbegriffen ausgewertet wird.

* 1. **Mögliche Erweiterungen: PGP (Pretty Good Privacy)**

Die Verschlüsselung der Nachrichten, dass nur der echte Empfänger sie lesen kann. Es werden Verschlüsselungsalgorithmen benützt, an denen sich selbst der amerikanische Geheimdienst die Zähne ausbeißt. Deshalb versuchten die USA den Export von PGP um jeden Preis zu verhindern. Zum Glück ist der Versuch gescheitert.

Herkömmliche Verfahren verwenden für das Codieren und Decodieren denselben Schlüssel. Dafür müssen Absender und Empfänger sich auf einen gemeinsamen Schlüssel einigen und diesen austauschen. Dies geschieht meistens unverschlüsselt. Ein Angreifer könnte dann alle weiteren Nachrichten mitlesen: Er hat ja den Schlüssel.

Im Gegensatz zu diesem symmetrischen Verfahren verwendet PGP eine asymmetrische Verschlüsselung. Dabei besitzt jeder Kommunkationspartner zwei Schlüssel: Einen privaten und einen öffentlichen. Den öffentlichen Schlüssel kann man beliebig verteilen. Mit dem öffentlichen Schlüssel kann man Nachrichten nur verschlüsseln, nicht aber 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))). In der Praxis wird man Nachrichten, wenn man sie verschlüsselt, zumeist auch signieren.

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.

Quellen:

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

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

<https://de.wikipedia.org/wiki/Google-Konto#Sicherheit>

<https://de.wikipedia.org/wiki/Gmail#Sicherheit>

<https://www.google.it/intl/de/about/company/security.html>

<http://www.zeit.de/digital/datenschutz/2016-10/google-kuenstliche-intelligenz-erfindet-eigene-verschluesselung/komplettansicht>

<https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/wozu.htm>

<https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/wasdas.htm>

[https://de.wikipedia.org/wiki/Pretty Good Privacy](https://de.wikipedia.org/wiki/Pretty%20Good%20Privacy)