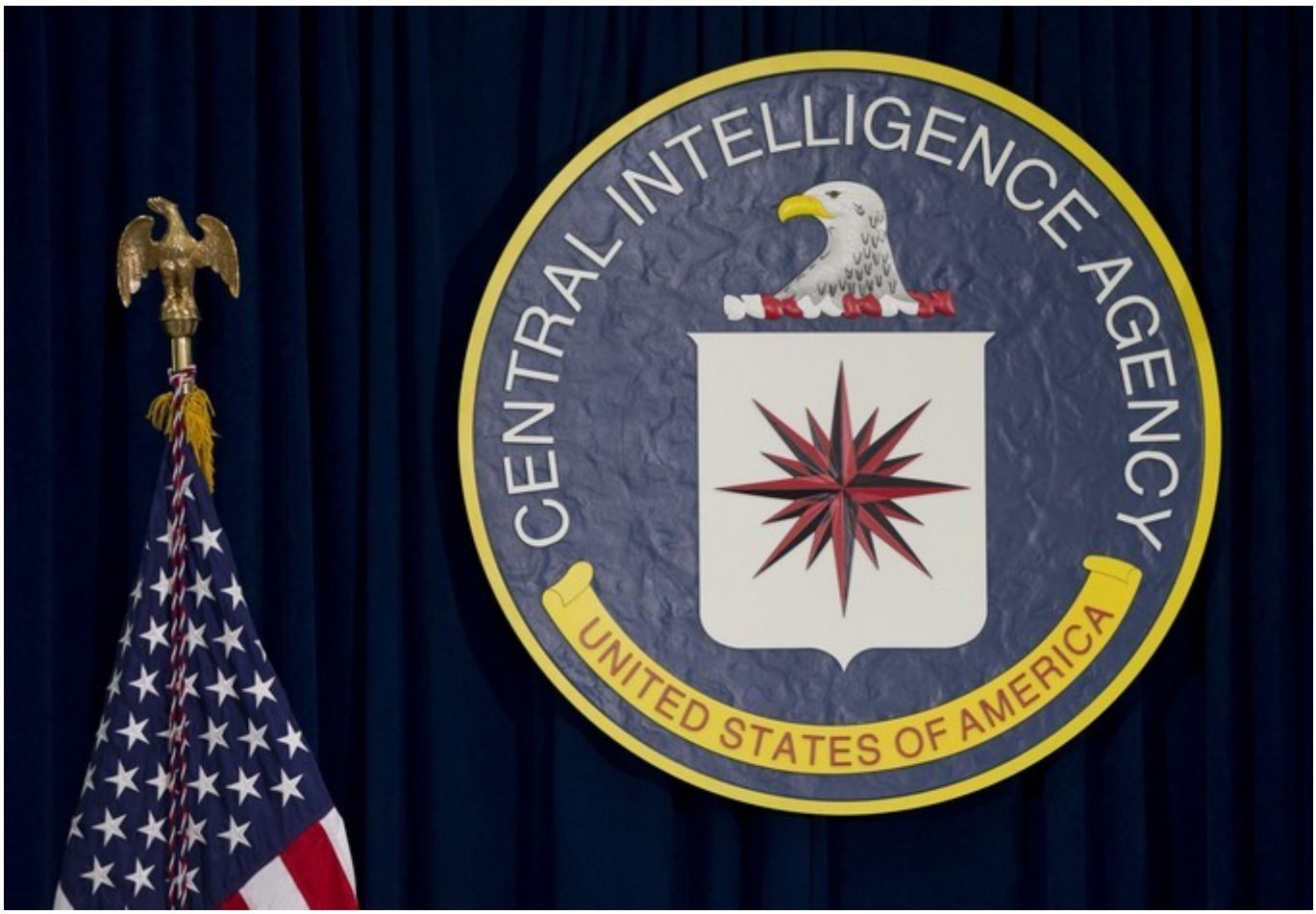
Die Wahrheit über Protonmail

Dieser Artikel ist am 28. August 2019 auf Englisch hier veröffentlicht worden:
https://privacy-watchdog.io/truth-about-protonmail/ heute jedoch nur noch im Webarchive:
https://web.archive.org/web/20210201234032/https://privacy-watchdog.io/truth-about-protonmail/

Er wurde – jedoch ohne die wichtigen Links - ins Deutsche übersetzt und hier publiziert:
https://de.stolenhistory.net/threads/die-wahrheit-%C3%BCber-protonmail.117/

Und schliesslich von mir mit den ursprünglichen Links zu den Quellen ergänzt:
Bearbeitet am 2. Okt 2021 von Dipl.-Ing. Andreas M. B. Groß, Morgarten/Innerschweiz

Inhaltsverzeichnis



1. Protonmail sieht aus wie ein CIA/NSA "Honeypot[1]"

Protonmail hat eine Onion-Domain[2], die es Nutzern ermöglicht, ihre Website mit dem TOR-Browser zu besuchen. Protonmail verfügt sogar über ein SSL-Zertifikat für diese Onion-Adresse, obwohl dies völlig unnötig ist. Wenn ein Benutzer ein neues Konto bei Protonmail über TOR einrichtet, wird er von Protonmails ".onion"-Adresse auf ".com" umgeleitet. Dadurch wird die sichere verschlüsselte Verbindung zur Onion-Adresse unterbrochen, was Ihre Identifizierung ermöglicht. Es gibt absolut keine technischen Gründe für diese Funktion. Tatsächlich sind die einzigen anderen Websites, die so arbeiten, mutmaßliche NSA/CIA-Honeypots.

Dies ist ein großes Sicherheitsproblem, das entweder dadurch entstanden ist, dass Protonmail von Teilchenphysikern verwaltet wird, die nichts von Computersicherheit verstehen, **oder** sie wurden gezwungen, ihre Website auf ähnliche Weise zu betreiben wie die Honeypots der CIA/NSA. Beide Möglichkeiten sind sehr bedenklich.

2. Protonmail bietet keine "Ende-zu-Ende-Verschlüsselung"

Professor Nadim Kobeissi hat mathematisch bewiesen, dass Protonmail keine Ende-zu-Ende-Verschlüsselung bietet[3]. Das bedeutet, dass Protonmail in der Lage ist, die Daten der eigenen Benutzer zu entschlüsseln. Als sich dies als wahr herausstellte, waren die Protonmail-Nutzer empört, dass sie belogen worden waren. Protonmail war gezwungen, eine öffentliche Erklärung abzugeben.[4] Die Erklärung beginnt so, wie man es erwarten würde: mit einem Seitenhieb auf den Sicherheitsforscher, der ihre Unredlichkeit aufgedeckt hat. Dann heißt es weiter: "Wir haben unsere Nutzer belogen, weil andere E-Mail-Unternehmen das auch getan haben"[5]. Keine Entschuldigung. Sie können die Daten ihrer Nutzer entschlüsseln, indem sie ihnen Skripte schicken, die ihnen dies ermöglichen. Sie werben jedoch damit, dass sie das nicht können. Das Eingeständnis von Protonmail[6] beweist, dass sie die gleiche Sicherheit bieten wie Gmail. Sowohl Gmail als auch Protonmail bieten eine Verschlüsselung an, die sie jederzeit entschlüsseln können.

3. Protonmail wurde unter Aufsicht der CIA/NSA entwickelt

Gmail und Protonmail wurden beide in von der CIA/NSA finanzierten Abteilungen unter deren Aufsicht entwickelt. Protonmail hat versucht, diesen Teil seiner Geschichte zu verbergen. Wir haben hier einen ganzen Artikel darüber geschrieben[7].

4. Protonmail ist teilweise im Besitz von CRV und der Schweizer Regierung

Nach einer erfolgreichen Crowdfunding-Kampagne mit dem Versprechen, "unabhängig zu bleiben", verkaufte Protonmail Aktienanteile[8] an CRV[9] und FONGIT[10]. Zum Zeitpunkt des Aktienverkaufs ar-

1 https://en.wikipedia.org/wiki/Honeypot_(computing)

2 https://web.archive.org/web/20210201234032/https://protonirockerxow.onion/

3 https://eprint.iacr.org/2018/1121.pdf

4 https://protonmail.com/blog/cryptographic-architecture-response/

5 Diesen Satz konnte ich so nicht in Protonmail‘s Rechtfertigung finden.

6 https://protonmail.com/blog/cryptographic-architecture-response/

7 https://web.archive.org/web/20210201234032/https://privacy-watchdog.io/protonmails-creation-with-cia-nsa/

8 https://protonmail.com/blog/protonmail-has-raised-2m-usd-to-protect-online-privacy/

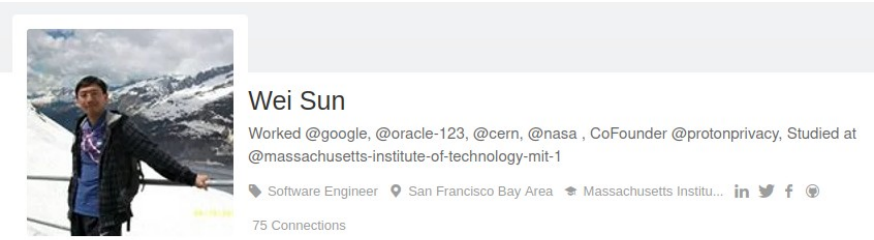
9 https://www.crv.com/

10 https://www.fongit.ch/about-us

beitete ein CRV-Gründer, Ted Ditersmith, für das US-Außenministerium in enger Zusammenarbeit mit Präsident Obama. Seine Position als Abgeordneter erforderte enge Kontakte zur CIA- und NSA-Verwaltung. Ted Ditersmith war auch Zeuge der Enthüllungen von Edward Snowden und erklärte, er wolle sein Unternehmenswissen zur "Terrorismusbekämpfung" einsetzen. FONGIT[11] ist eine Non-Profit-Organisation, die von der Schweizer Regierung finanziert wird[12]. Der Mitarbeiter von Protonmail, Antonio Gambardella, arbeitet ebenfalls für die Schweizer Regierung[13].

5. CRV, In-Q-Tel und die CIA

Die CIA betreibt offen eine Scheinfirma, In-Q-Tel[14], deren erklärter Zweck es ist, im Auftrag der CIA in Technologieunternehmen zu investieren. In-Q-Tel hat erklärt, dass sie ein besonderes Interesse an den in E-Mails[15] und verschlüsselter Kommunikation enthaltenen Informationen haben. Es hat sich gezeigt, dass In-Q-Tel die Brücke zwischen der CIA und Gmail ist[16]. Eine Analyse der Mitarbeiter zeigt Verbindungen zwischen CRV und In-Q-Tel. Die US-Medien bestätigen diese Verbindungen, wenn sie CRV interviewen[17], damit sie In-Q-Tel verstehen können. Darüber hinaus arbeitet Wei Sun, der Vordenker, Kryptograph und Backend-Entwickler, der Protonmail entwickelt hat, jetzt für Google[18].



6. Protonmail folgt den Anforderungen der CIA an E-Mail-Format und Metadaten

Durchgesickerte Dokumente bei Wikileaks zeigen, dass die CIA verlangt, dass E-Mails als EML-Dateityp gespeichert werden. Es gibt mehrere Möglichkeiten, E-Mails zu speichern, und Protonmail hat das von der CIA geforderte Format gewählt. Protonmail bietet keinen Schutz für die Metadaten der Benutzer und hat offiziell erklärt, dass sie die Metadaten an die Strafverfolgungsbehörden weitergeben. Edward Snowden hat aufgedeckt, dass sich die US-Regierung am wenigsten um den Inhalt von E-Mails kümmert. Snowden enthüllte, dass sich die US-Strafverfolgungsbehörden am meisten dafür interessieren, mit wem eine Person spricht, das Datum und die Uhrzeit der E-Mails sowie den Betreff der E-Mail. Die Verschlüsselung von Betreff und Metadaten ist nicht schwer zu bewerkstelligen. Protonmail weigert sich jedoch, Daten zu schützen, die für die CIA und das FBI am wertvollsten sind, und speichert sie im Klartext (ohne Verschlüsselung). Edward Snowden erklärte, dass die NSA "nicht in der Lage ist, die Verschlüsselungsalgorithmen zu kompromittieren, die diesen Technologien zugrunde liegen. Stattdessen umgeht oder untergräbt sie sie, indem sie Unternehmen

11 https://www.fongit.ch/about-us

12 https://www.fongit.ch/about-us

13 https://protonmail.com/about

14 https://en.wikipedia.org/wiki/In-Q-Tel

15 https://web.archive.org/web/20210223155504/https://www.nytimes.com/2001/12/30/business/suddenly-uncle-sam-wants-to-bankroll-you.html Suddenly, Uncle Sam Wants to Bankroll You

16 https://medium.com/insurge-intelligence/how-the-cia-made-google-e836451a959e

17 https://web.archive.org/web/20210223155504/https://www.nytimes.com/2001/12/30/business/suddenly-uncle-sam-wants-to-bankroll-you.html Suddenly, Uncle Sam Wants to Bankroll You

18 https://angel.co/u/wei-sun-7

zur Zusammenarbeit zwingt[19]. Protonmail hat sich geweigert, die von der NSA gewünschten Informationen zu schützen, was Anlass zur Sorge gibt.

7. Das Schweizer MLAT-Gesetz könnte der NSA vollen Zugang verschaffen

Die Server von Protonmail befinden sich in der Schweiz, einem Land mit einem MLAT-Abkommen, das es der NSA ermöglichen könnte, weiterhin "fast alles" über die Internetkommunikation einer Person aufzuzeichnen. Jegliche Zweifel an der Anwendbarkeit des MLAT-Abkommens werden ausgeräumt, wenn man bedenkt, dass Protonmail zum Teil im Besitz von FONGIT ist, einem von der Schweizer Regierung finanzierten Unternehmen. Protonmail hat außerdem vor kurzem seine Datenschutzrichtlinien überarbeitet[20] [21], um Formulierungen und Anforderungen des MLAT-Abkommens aufzunehmen. Ihr Vorgehen zeigt, dass sie vor dem MLAT-Abkommen kapitulieren. Zu den Überarbeitungen gehört eine Änderung der Datenschutzrichtlinie, die es ihnen erlaubt, Ihren Standort zu verfolgen, während Sie ihren Dienst in einigen Situationen nutzen.

8. Protonmail nutzt Radware für DNS/DDOS-Schutz

Datenschutzunternehmen wie Protonmail müssen wegen der häufigen Angriffe auf ihren Dienst einen DNS/DDOS-Dienst nutzen. Protonmail nutzt zu diesem Zweck ein Unternehmen namens Radware[22]. Radware ist ein minderwertiger Dienst, der keinen angemessenen Schutz bietet. Protonmail wurde offline genommen, manchmal von Teenagern[23], weil sie darauf bestanden, einen minderwertigen Dienst zu nutzen. Es ist erwähnenswert, dass das internationale Büro von Radware nur wenige Kilometer vom Hauptsitz des mächtigsten Geheimdienstes der Welt, dem israelischen Mossad, entfernt ist. Radware kann sich auf zwei Arten vollständigen Zugriff auf alle Protonmail-Benutzerkonten verschaffen. Sie könnten einige Codezeilen einschleusen, die den Benutzernamen und das Kennwort aller Benutzer preisgeben und es ihnen so ermöglichen, sich so anzumelden, als wären sie der betreffende Benutzer. Sie könnten auch Benutzernamen und Passwörter von Protonmail erhalten. Zur Erinnerung: Protonmail hat zugegeben, dass sie auf alle Benutzerkonten zugreifen und deren Daten entschlüsseln können. Außerdem wurde berichtet, dass Radware direkte Verbindungen zu den israelischen Verteidigungskräften hat[24].

9. Protonmail-Entwickler verwenden Protonmail nicht

Die Entwickler von Protonmail sind in der Lage, die tatsächliche Sicherheit von Protonmail zu kennen. Und die Entwickler von Protonmail benutzen Protonmail nicht[25]. Wenn Sie ein Essen von einem Koch serviert bekämen, der sich weigert, das Essen zu essen, wäre das für Sie ein Grund zur Sorge? Dies ist die gleiche Situation. Die Protonmail-Entwickler verwenden Protonmail nicht, und dafür gibt es wahrscheinlich gute Gründe.

10. Protonmail beteiligt sich an illegaler Cyberkriegsführung

Im Jahr 2017 scheint Protonmail illegale Cyberkriegsführungsfähigkeiten eingesetzt zu haben, um

19 https://mashable.com/archive/snowden-nsa-break-internet-encryption

20 https://www.reddit.com/r/privacy/comments/cwld9o/protonmail_changed_his_policy/eykbrqz/

21 https://protonmail.com/privacy-policy

22 https://protonmail.com/support/knowledge-base/protonmail-israel-radware/

23 https://techcrunch.com/2018/09/06/protonmail-names-one-of-the-attackers-behind-a-major-ddos-this-summer/

24 https://cryptome.org/2015/11/protonmail-ddos.htm

25 https://web.archive.org/web/20210127135328/https://privacy-watchdog.io/protonmail-devs-do-not-use-protonmail/

unrechtmäßig in einen verdächtigen Server einzubrechen[26]. Sie können den geposteten Tweet sehen und hier darüber lesen[27]. Sie löschten den Tweet bald darauf und sagten: "Wir können weder bestätigen noch dementieren, dass etwas passiert ist." Im Jahr 2013 stimmte das EU-Parlament dafür, Hacken zu einer Straftat zu machen, die mit einer Gefängnisstrafe von 2 Jahren geahndet wird[28]. Das "Zurückhacken" ist auch nach Schweizer Recht illegal. Allein aufgrund der Eingeständnisse von Protonmail hat das Unternehmen einen illegalen Hack durchgeführt.

11. Protonmail hat sich oft unehrlich verhalten

Seit der Gründung von Protonmail wurden die Benutzer belogen[29]. Angefangen bei der Crowdfunding-Aktion für 550.000 Dollar, um "unabhängig zu bleiben", ein Versprechen, das sie fast sofort brachen, indem sie Anteile an ein US-Unternehmen verkauften, das Verbindungen zu Präsident Obama und John Podesta hat[30].

Unserer Meinung nach ist Protonmail keine E-Mail-Lösung, die Sie verwenden sollten, wenn Sie Privatsphäre oder Sicherheit wünschen. Ihre E-Mails werden wahrscheinlich in einem US-Rechenzentrum direkt neben Ihren Gmail-E-Mails landen.

Privacy Watchdog

# # #

26 https://www.vice.com/en/article/qvvke7/email-provider-protonmail-says-it-hacked-back-then-walks-claim-back

27 https://www.vice.com/en/article/qvvke7/email-provider-protonmail-says-it-hacked-back-then-walks-claim-back

28 https://www.reuters.com/article/net-us-eu-cybercrime-idUSBRE9630LD20130704

29 https://web.archive.org/web/20210127135330/https://privacy-watchdog.io/protonmails-false-claims/

30 https://web.archive.org/web/20210127135333/https://privacy-watchdog.io/protonmails-crowdfunding-equity-sale/