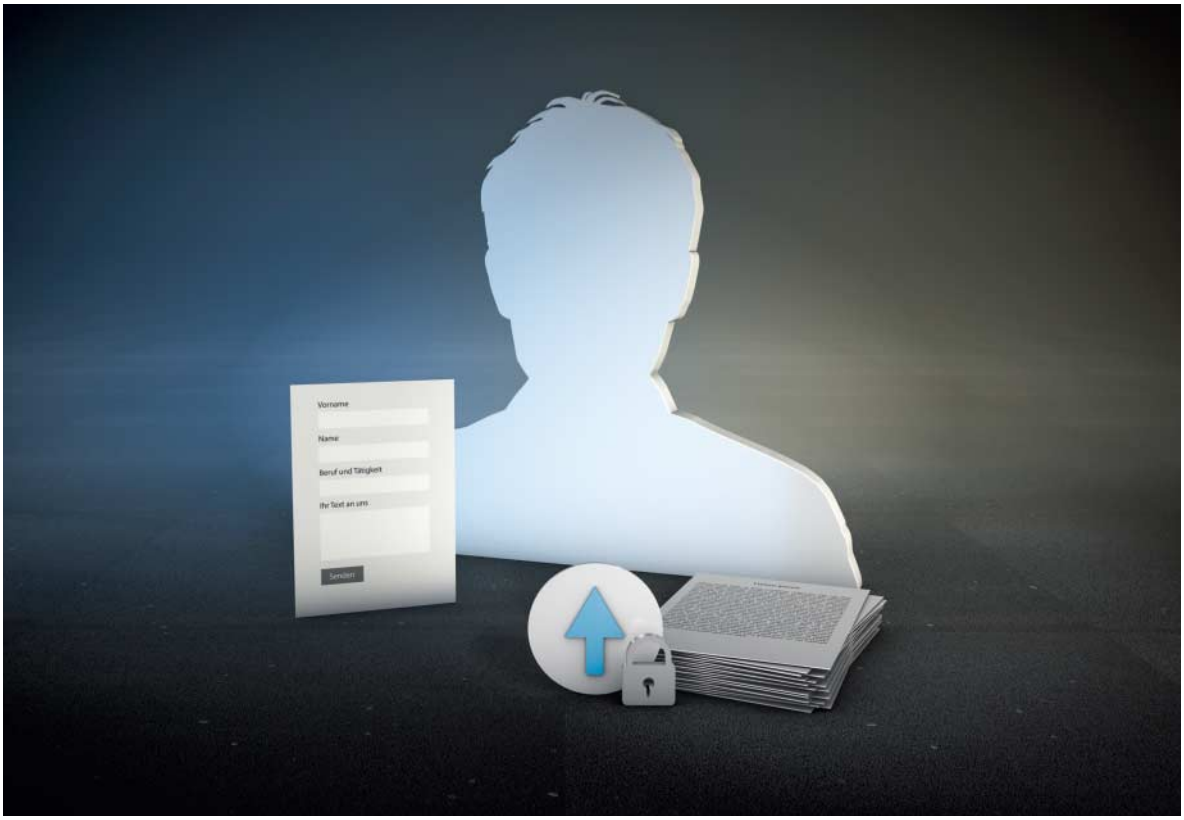


Einfach / sicher

Hinter den Kulissen von heise Tippgeber

Die Webseiten zum heise Tippgeber sind bewusst schlicht und selbsterklärend. Wenn Sie etwas genauer wissen wollen, wie das alles hinter den Kulissen funktioniert, sind Sie hier an der richtigen Stelle.

Von Jürgen Schmidt

Wenn Sie **https://heise.de/tippgeber** aufrufen, landen Sie auf der Einstiegsseite unseres anonymen Briefkastens. Sie bietet Ihnen zwei Optionen: das anonyme Kontaktformular und den sicheren Briefkasten. Beide sind auf Sicherheit optimiert – allerdings mit einem jeweils anderen Schwerpunkt.

Das anonyme Kontaktformular bietet Ihnen die Möglichkeit, uns sofort und ohne Angabe Ihres Namens oder einer E-Mail-Adresse brisante Informationen zu übermitteln; das ist maximal einfach und schon recht sicher umgesetzt. Der sichere Briefkasten hingegen ist auf bestmöglichen Schutz Ihrer Anonymität und der übermittelten Daten optimiert; seine Nutzung erfordert aber etwas Vorarbeit.

Auch beim einfachen Kontaktformular haben wir viel Mühe darauf verwendet, so gut wie möglich zu gewährleisten, dass weder die übermittelten Informationen noch das Wissen über deren Herkunft in die falschen Hände geraten. So liefert ein eigener kleiner HTTPS-Server die Web-Seiten des anonymen Kontaktformulars aus und nimmt die Daten entgegen. Dessen Seiten binden keine Ressourcen von externen Quellen ein; insbesondere befinden sich in ihnen weder Werbung noch Zählpixel, die Dritten Hinweise auf Ihre Whistleblower-Aktivitäten liefern könnten.

Die von Ihnen in das Formular eingegebenen Informationen werden schon im Browser mit PGP verschlüsselt und dann erst an den Server und von diesem via Mail an das Investigativ-Team von c’t geschickt. Die PGP-Verschlüsselung umfasst alle Informationen, die Sie im Formular eintragen – also auch Betreff und den optionalen Namen beziehungsweise die ebenfalls optionale E-Mail-Kontaktadresse.

Den zur Entschlüsselung benötigten geheimen Schlüssel haben nur ausgewählte Redakteurinnen und Redakteure. Diese werden das ankommende Material täglich sichten, bewerten und dann in aller Regel an mit dem Thema befasste Redakteure weitergeben. Besonders brisantes Material wird unter Umständen auch innerhalb des Investigativ-Teams bearbeitet.

Die Verschlüsselung erfolgt noch vor der Übertragung schon bei Ihnen im Browser über die JavaScript-Bibliothek openpgp.js. Wenn Sie JavaScript abgeschaltet haben, entfällt die PGP-Verschlüsselung und die Informationen werden lediglich durch die Transportverschlüsselung TLS geschützt.

Die Einfachheit bringt aber zwei Nachteile mit sich. Zum einen können Sie uns über das anonyme Kontaktformular keine Dateien zusenden. Als Workaround können Sie etwa mit 7zip ein verschlüsseltes ZIP-Archiv erstellen und mit einem neutralen Namen bei einem One-Click-Hoster wie transfer.sh hochladen. Uns schicken Sie dann über das Kontaktformular die Download-URL und das Passwort. Der Upload-Server sieht dabei aber natürlich Ihre IP-Adresse, die Im Zweifelsfall zu Ihnen führen kann.

Damit kommen wir auch schon zum zweiten Nachteil der simplen HTTPS-Lösung: Auch wir sehen Ihre IP-Adresse. Sie wird auf den Heise-Servern protokolliert und gemäß unserer Privacy Policy spätestens nach 7 Tagen gelöscht. Wir haben diskutiert, das Logging abzuschalten, das aber verworfen, weil wir in der Praxis nicht garantieren können, dass die Daten innerhalb des Heise-Clusters mitgelesen und gespeichert werden. Sie müssen also den Heise-Admins vertrauen, und zwar gleich in zweierlei Hinsicht: Erstens, dass sie sich selber nicht an diesen Daten vergreifen, und zweitens, dass sie ihre Server so sauber halten, dass Dritte nicht an die IP-Adressen rankommen.

Die Gefahr eines solchen Missbrauchs ist gering und das Risiko dürfte in vielen Fällen tragbar sein. Trotzdem waren wir damit nicht zufrieden. Unser Anspruch ist es, eine Anlaufstelle zu bieten, die Ihre Anonymität und die übermittelten Daten bestmöglich schützt.

Wer sich besonders gut schützen möchte, könnte auf die Idee verfallen, das anonyme Kontaktformular mit dem Tor-Browser über das Anonymisierungs-Netz Tor zu nutzen. Zwar bekommen wir dabei Ihre IP-Adresse nicht mehr zu sehen, doch dafür läuft die gesamte Kommunikation über Tor-Exit-Nodes, die unter anderem von Geheimdiensten betrieben werden, um dort Daten abzugreifen. Und gegen deren gezielte Angriffe bietet die Transportverschlüsselung via HTTPS keinen ausreichenden Schutz. Deshalb raten wir davon ab.

Tails, Tor und Secure Drop

Deshalb haben wir den sicheren Briefkasten für heise Tippgeber entworfen. Er setzt auf das Open-Source-Projekt Secure Drop auf. Es wurde speziell für eine sichere Kommunikation zwischen Whistleblowern und Journalisten entwickelt und ist auf allerhöchste Sicherheit ausgelegt. Unter anderem The Guardian, die Washington Post und The Intercept benutzen Secure Drop.

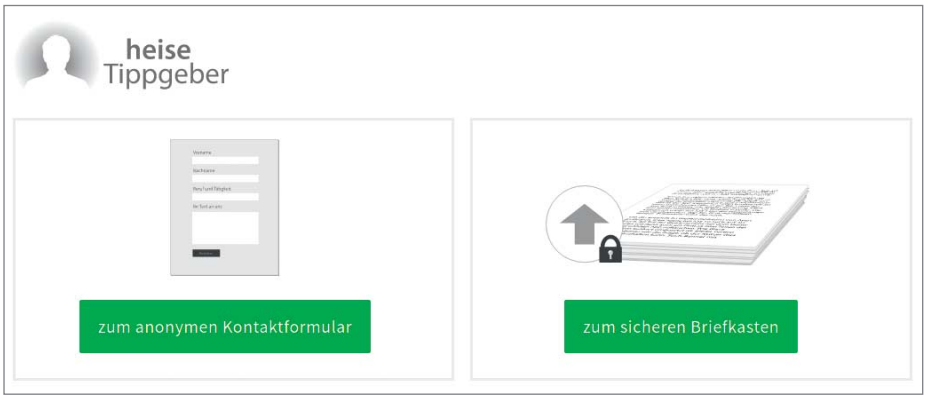
Secure Drop setzt voll auf das Anonymisierungsnetz Tor. Dabei ist ein Secure-Drop-Server nicht im normalen Web, sondern nur als sogenannter Hidden Service innerhalb des Tor-Netzes über eine .onion-Adresse erreichbar. Um ihn zu besuchen, müssen Sie also zumindest den Tor-Browser installieren; wie das geht, wird auf den Seiten von heise Tippgeber erklärt. Vorsichtige Naturen gehen sogar noch einen Schritt weiter und nutzen das auf Anonymität und Sicherheit optimierte Live-Linux-System Tails (siehe Tipp 8 auf Seite 128).

Ein Secure-Drop-Briefkasten hat mehrere Vorteile gegenüber einem reinen HTTPS-Dienst. So hat der Betreiber keine Möglichkeit, Zugriffe zurückzuverfolgen. Darüber hinaus garantiert ein Hidden Service innerhalb des Tor-Netzes auch noch eine vertrauenswürdige Ende-zu-Ende-Verschlüsselung zwischen dem Dienst und dem Tor-Browser des Whistleblowers, die zuverlässiger schützt als TLS. Das bedeutet, dass anders als bei der herkömmlichen Tor-Nutzung mit den Exit-Nodes keines der Systeme, das die Daten befördert, diese mitlesen kann, solange Sie die richtige Onion-Adresse verwenden. Um ganz sicher zu gehen, nehmen Sie am besten die im c't-Impressum abgedruckte .onion-URL.

Secure Drop ist jedoch mehr als Tor; es definiert eine hochsichere Gesamt-Architektur. Das beginnt damit, dass der Hidden Service selbst auf einem speziell gehärteten Linux-System aufsetzt, das von einem ebenfalls gehärteten, unabhängigen Monitoring-System permanent überwacht wird, um mögliche Angriffe zu erkennen. Die beiden Server unseres sicheren Briefkastens stehen in einem abgeschlossenen Raum im Heise-Verlag (also nicht in einem externen Rechenzentrum), zu dem nur ausgewählte Personen Zugang haben, und hängen in einem eigenen Netz.

Ankommende Daten verschlüsselt der Secure-Drop-Server sofort mit einem dort hinterlegten PGP-Schlüssel. Der zum Entschlüsseln erforderliche geheime Schlüssel, der sogenannte Viewing-Key, ist nicht auf dem Server vorhanden. Somit kann ein Angreifer, der den Server kapert oder komplett beschlagnahmt respektive klaut, die dort abgelegten Informationen nicht lesen.

Um Zugriff auf die im Briefkasten eingeworfenen Dokumente zu erlangen, muss sich eine der dazu berechtigten Personen am Journalisten-Zugang des Secure-Drop-Servers anmelden. Dies erfolgt ebenfalls via Tor von einem gesicherten, speziell zu diesem Zweck von einem USB-Stick gestarteten Tails-System. Der Login ist über eine Drei-Faktor-Authentifizierung abgesichert. Erstens muss sich das Tails-System gegenüber dem Secure-Drop-Service mit einem Token ausweisen, um überhaupt mit



heise Tippgeber bietet zwei Optionen: das einfach zu benutzende, anonyme Kontaktformular und den hochsicheren Briefkasten.

dem Journalisten-Zugang reden zu dürfen. Dann muss der Journalist ein Passwort eingeben. Und als Drittes muss er ein temporäres Einmal-Passwort vorweisen, das etwa der Google Authenticator auf seinem Smartphone erzeugt.

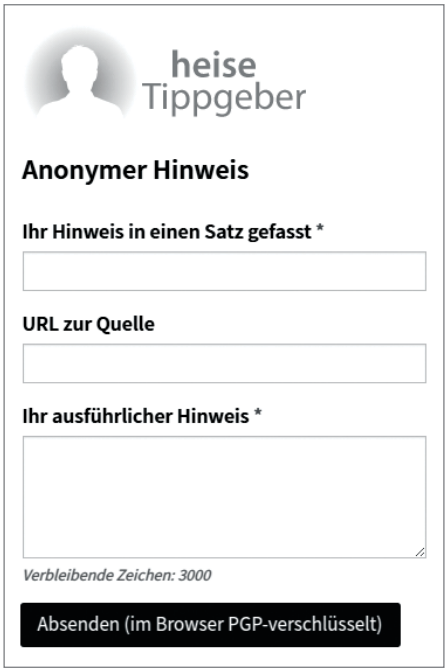
Damit kann er dann die Daten auf sein Journalisten-Tails-System herunterladen – immer noch PGP-verschlüsselt wohlgemerkt. Gemäß der reinen SecureDrop-Lehre könnte er diese Daten dort immer noch nicht entschlüsseln, sondern müsste sie zunächst auf einen zweiten USB-Stick speichern. Den trüge er dann zu einer speziellen Viewing-Station in einem sicheren Raum und ohne Netzwerk-Verbindung. Nur diese Offline-Viewing-Station hätte den erforderlichen Viewing-Key, um die Whistleblower-Dokumente zu entschlüsseln.

Diese letzte Stufe haben wir uns jedoch nach reiflicher Überlegung gespart. Bei heise Tippgeber findet sich der Viewing-Key direkt innerhalb des gesicherten Tails-Systems der Mitglieder des Investigativ-Teams – nicht auf deren Arbeitsplatz, sondern im verschlüsselten Bereich eines gehärteten Systems, das nur zu diesem Zweck genutzt wird.

Der eingesparte Umweg über die Viewing-Station erleichtert eine zeitnahe Sichtung und Bearbeitung des übermittelten Materials enorm. Den Ausschlag für diesen Sicherheitskompromiss gab die Einschätzung, dass jemand, der einem Journalisten seinen Stick abnehmen und ihn zur Herausgabe seines Passworts nötigen kann, wohl ohne großen Mehraufwand auch die Viewing-Station in seinen Besitz bringen könnte. Dieses Angriffszenario erschien uns auch deutlich realistischer als eine Kompromittierung des Journalisten-Tails-Systems etwa durch ein BIOS-Rootkit oder einen gezielten Angriff übers Netz.

Ein wichtiger Aspekt des SecureDrop-Konzepts ist, dass es sichere Arbeitsabläufe fördert. Die heruntergeladenen Dokumente hinterlassen in der Heise-Infrastruktur keine Spuren – weder auf dem Arbeitsplatz-System des Bearbeiters noch in Monitoring-Systemen des verwendeten Netzes. Die Daten werden über die Ende-zu-Ende-verschlüsselte Tor-Verbindung heruntergeladen und landen damit in dem nur über Tor mit dem Internet verbundenen Journalisten-Tails. Dort kann der Bearbeiter die Daten entschlüsseln, sichten und in einem verschlüsselten Bereich des USB-Sticks dauerhaft aufbewahren.

Wenn er die Daten dort löscht beziehungsweise erst gar nicht im verschlüsselten, permanenten Bereich speichert, sind sie nach menschlichem Ermessen weg, ohne irgendwelche Spuren zu hinterlassen, die ihr ehemaliges Vorhandensein oder auch nur den Kontakt dokumentierten. Erst wenn der Journalist zu der Überzeugung gelangt, dass es die Gefahrenlage zulässt, wird er die Daten etwa über einen zweiten USB-Stick auf seinen Arbeitsplatz befördern, um sie schließlich in einen Artikel einfließen zu lassen. Dazu wird er typischerweise die exportierten Daten vorher noch anonymisieren, indem er



Die über das Kontaktformular verschickten Daten werden zusätzlich PGP-verschlüsselt.

Meta-Informationen oder unerwünschten Personenbezug entfernt. So landen sensible Informationen nie im Klartext auf ungesicherten Systemen.

Schließlich ermöglicht Secure Drop auch eine Kommunikation zwischen Whistleblower und Journalist, ohne dass die beiden direkten Kontakt hätten. Dazu erhält jeder Tippgeber bei seinem ersten Besuch einen Geheimcode, den er sich merken oder aufschreiben und sicher verwahren muss. Bei weiteren Besuchen sieht er nach dessen Eingabe eventuelle Antworten oder Rückfragen des Journalisten und kann dann auch weitere Informationen nachreichen.

Diese zugegebenermaßen etwas längliche Beschreibung des nicht sichtbaren Teils von heise Tippgeber soll dokumentieren, dass für uns die Sicherheit der übermittelten Daten und des Tippgebers nicht bei einer verschlüsselten Upload-Möglichkeit aufhört. Wir unternehmen tatsächlich alles in unserer Macht Stehende, um auch danach einen verantwortungsvollen Umgang mit den von Ihnen bereitgestellten Informationen sicherzustellen. Fassen Sie sich also ein Herz und lassen Sie uns Informationen zu Missständen zukommen, die schon lange an Ihrem Gewissen nagen. *(ju@ct.de)* c't

Secure Drop im Tor-Netz

Das Anonymisierungsnetz Tor sichert die Übertragung und verhindert das Zurückverfolgen.