Vorhang auf

Die neue Enthüllungsplattform heise Tippgeber

Wir als c't und Heise-Verlag bieten Ihnen ab sofort eine neue Möglichkeit, uns brisante Informationen zuzuspielen: Die heise-Tippgeber-Plattform dokumentiert, dass wir gewillt sind, uns das dafür nötige Vertrauen zu verdienen.

Von Jürgen Schmidt

Wer einen Missstand aufzeigen und anprangern will, braucht dafür eine geeignete Plattform. Der Heise-Verlag hat unter anderem mit c't und heise online eine große Sichtbarkeit im deutschsprachigen Raum und ein Renommee für seriöse, verantwortungsvolle Berichterstattung. Darüber hinaus haben die Redaktionen und insbesondere deren investigativ arbeitende Redakteure den erforderlichen technischen Sachverstand, um mit Informationen sicherheitsbewusst umzugehen. Der ab sofort auf heise online erreichbare heise Tippgeber ist unser Angebot, uns brisantes Material sicher zu übermitteln.

Sie erreichen den heise Tippgeber über die Kontakt-Option auf der Startseite von heise Online oder direkt via **https://heise.de/tipps**. Diese Adresse findet sich ab sofort auch im Impressum jeder c't-Ausgabe. Die Webseiten dazu sind (hoffentlich) selbsterklärend. Sie können dort zwischen einem gut gesicherten, anonymen Kontaktformular und unserem bestmöglich abgesicherten Briefkasten wählen. Beide erlauben eine anonyme Kontaktaufnahme zur Redaktion. Details zu Konzept und Funktionsweise liefert der Artikel ab Seite 130.

Nutzen Sie den heise Tippgeber, um uns auf Missstände aufmerksam zu machen und uns dabei auch die Mittel an die Hand zu geben, darüber zu berichten. Sie können uns einfache Hinweise, vertrauliche Unterlagen, Verträge, Fotos, E-Mail-Verkehr oder auch Datenbankauszüge zu-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

kommen lassen. Je besser die Informationen die Sachlage demonstrieren und belegen, desto besser können wir diese einschätzen und über unser weiteres Vorgehen in dieser Sache entscheiden.

Wir sind darauf vorbereitet, brisantes Material entgegenzunehmen und angemessen zu behandeln. So ist etwa sichergestellt, dass selbst eine Beschlagnahmung oder ein Diebstahl von PCs und Servern im Heise-Verlag keinen Zugang zu diesen Informationen oder deren Quelle ergäben (Details dazu, wie wir das verhindern, verrät der Artikel ab Seite 130). Und wir werden mit diesen Informationen verantwortungsvoll umgehen. Das bedeutet insbesondere, dass wir uns zugespielte Informationen in aller Regel nicht unbearbeitet veröffentlichen werden.

Dass wir die Fakten auf Richtigkeit checken und unter anderem durch weitere Recherchen in einem angemessenen Kontext präsentieren, versteht sich von selbst – das ist Teil unserer tagtäglichen Arbeit. Darüber hinaus werden wir die Informationen vor einer Veröffentlichung so aufbereiten, dass sie zwar den fraglichen Sachverhalt deutlich darlegen, dabei aber keine Kollateralschäden bei Unschuldigen verursachen oder Rückschlüsse auf unsere Quelle ermöglichen.

Pro und Contra Anonymität

Der heise Tippgeber ermöglicht vollständig anonyme Kontakaufnahme und Informationsübergabe. Wir respektieren den Wunsch unserer Quellen, auch uns gegenüber anonym zu bleiben und stellen deshalb eine Plattform bereit, die Informationen wie die IP-Adressen der Absender gar nicht erst zu sehen bekommt. Wir haben damit schon technisch keine Möglichkeit mehr, eine Kontaktaufnahme zurückzuverfolgen. Wenn Sie es uns nicht verraten, wissen wir nicht, mit wem wir es zu tun haben.

Das heißt jedoch keineswegs, dass wir die anonyme Kommunikation bevorzugen. Im Gegenteil: In vielen Fällen ist es sinnvoller, wenn Sie uns als Tippgeber Ihre Identität offenlegen. Das gilt auch und gerade, wenn Sie verhindern wollen, dass etwa Strafverfolgungsbehörden oder rachsüchtige Geschädigte Kenntnis darüber erlangen.

Denn wir schützen unsere Quellen und überlassen das keineswegs nur dem Tippgeber selbst. Und wenn wir wissen, wen und was wir zu schützen haben, können wir das besser. So können wir etwa das Risiko, dass eine Veröffentlichung auf eine bestimmte Person zurückzuführen ist, besser einschätzen, wenn wir diese Person und das Umfeld kennen, aus dem ein Dokument stammt.

Es mag sogar vorkommen, dass wir die Gefahr einer Zurückverfolgung auf Grund unserer Erfahrungen mit gezielter Recherche besser einschätzen können als der Tippgeber selbst. Mit diesem Wissen können wir die Informationen vor der Veröffentlichung so aufbereiten, dass sie eben nicht mehr mit einem großen Pfeil auf den Tippgeber zeigt. Im Extremfall würden wir sogar von einer Veröffentlichung abraten und auf Berichterstattung verzichten.

Presse genießt in Deutschland einen besonderen Status. So garantiert Artikel 5 des Grundgesetzes die Pressefreiheit und schützt dabei ausdrücklich den gesamten Prozess von der Beschaffung einer Information über die Produktion bis hin zur Verbreitung von Nachrichten.

Der heise Tippgeber – die Charta

Der heise Tippgeber ist eine vertrauenswürdige Anlaufstelle für Whistleblower im deutschsprachigen Raum. Er ist ein Angebot an alle Menschen, die auf Missstände hinweisen und dabei anonym bleiben wollen.

Unser Versprechen

1. Wir tun unser Möglichstes, um Schaden von unseren Tippgebern fernzuhalten. Insbesondere tun wir alles in unserer Macht Stehende, um deren Anonymität zu bewahren.
2. Wir gehen verantwortungsvoll mit den uns übermittelten Informationen um, um Schaden von Unschuldigen fernzuhalten.

Was für Informationen kann ich übermitteln und was geschieht dann damit?

Wenn Sie Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns anonym interne Papiere, Verträge, Fotos, Datenbankauszüge und andere Daten übermitteln. Wir werden die Informationen zunächst auf Relevanz und Korrektheit prüfen; dies geschieht durch erfahrene Redakteurinnen und Redakteure. Dann erst entscheiden wir, ob und wie wir diese Informationen weiterverwenden. Im Fall von hoch brisanten und vielleicht sogar gefährlichen Informationen sind wir darauf vorbereitet, diese angemessen weiterzubearbeiten – also unter anderem sicherzustellen, dass diese Informationen nicht in falsche Hände geraten.

In aller Regel werden wir zugespielte Informationen nicht einfach veröffentlichen. Sie geben vielmehr den Anstoß zu weiteren Recherchen, die letztlich in eine Veröffentlichung münden können. Diese erfolgt dann nach allen Regeln der journalistischen Sorgfaltspflicht, was insbesondere bedeutet, dass Ihre Informationen journalistisch bearbeitet werden.

Der heise Tippgeber versteht sich als anonymer Briefkasten des Heise-Verlags. Eine Veröffentlichung kann in allen Medien des Heise-Verlags erfolgen – etwa im Rahmen von heise online, c't, iX, heise Security oder Telepolis.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Die Redakteure des Investigativ-Teams nutzen speziell gesicherte Systeme, um den sicheren Briefkasten zu leeren.

Redakteure sind damit professionelle Geheimnisträger und haben auch gegenüber Strafverfolgungsbehörden und vor Gericht ein spezielles Zeugnisverweigerungsrecht, das wir nutzen werden, um Schaden von unseren Tippgebern fernzuhalten. Insbesondere werden wir dessen Identität, auch wenn sie uns bekannt ist, nicht an Dritte weitergeben.

Es bleibt natürlich ein Restrisiko, dass uns ein Richter durch Beugehaft zur Herausgabe der Identität unserer Quellen zwingt (siehe den Artikel zum Quellenschutz auf S. 134). Nach unserer Einschätzung sind wir in Deutschland nicht so weit, dass das ein realistisches Szenario wäre. Doch einem Auftragsmörder, der uns ganz real eine Pistole an die Schläfe hält, würden wir unser geheimes Passwort, das die Informationen schützt, dann wohl doch preisgeben. Wenn Sie also damit rechnen, sollten Sie den vollständig anonymen Weg über unseren sicheren Briefkasten wählen.

Aber sicher

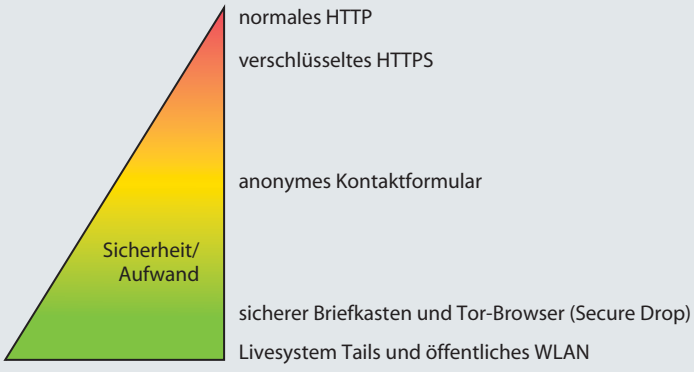
Vielleicht noch wichtiger als die optionale Anonymität gegenüber der Redaktion ist die Tatsache, dass der heise Tippgeber Ihnen beste Voraussetzungen für eine sichere Kontaktaufnahme, Kommunikation und Übermittlung von Informationen bereitstellt.

Allerdings können wir Ihnen dabei das mit der Sicherheit nicht vollständig abnehmen. Wenn Sie sicherstellen wollen, dass weder die Daten noch Informationen zu Ihrer Identität in falsche Hände geraten, müssen auch Sie etwas dafür tun. Dabei sollten Sie Ihre Vorkehrungen der möglichen Gefahr anpassen: Die fallen dann natürlich anders aus, je nachdem, ob ein öffentlich bloßgestellter Chef, ein gewalttätiger Mafia-Pate oder Strafverfolger hinter Ihnen her sind.

Wir haben auf der folgenden Seite 10 Tipps für Tippgeber zusammengestellt, die nach Sicherheitsgewinn und Aufwand sortiert sind. Daran können Sie sich orientieren und das Richtige für Ihre Situation herauspicken. Hoffentlich haben Sie all diese Erklärungen zu Gefahren und notwendigen Vorkehrungen nicht davon abgeschreckt, das Richtige™ zu tun. Wir warten jedenfalls auf Ihren Tipp. *(ju@ct.de)* c't

Aufwand versus Sicherheit

Wer seine Identität und brisante Daten besonders schützen will, muss zusätzlichen Aufwand betreiben. Der eigene Schutzbedarf bestimmt, wie viel.



© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Anzeige

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

10 Tipps für Tippgeber

Bei der Sicherheit für Whistleblower gibt es keine universellen Ratschläge; man muss seine Vorkehrungen an den eigenen Bedarf anpassen, ohne dass es dabei allzu unbequem wird. Das gilt auch für die folgenden Tipps für Tippgeber.

1 . Security-Basics beachten

Grundvoraussetzung ist ein sicheres und sauberes System; nutzen Sie Antiviren-Software und halten Sie System und Anwendungen auf dem aktuellen Stand.

2. Nicht im Firmen-Netz

Es ist eine schlechte Idee, Informationen oder Daten von Ihrem Arbeitsplatz oder überhaupt aus dem Netz Ihrer Firma zu verschicken. Sie hinterlassen dabei immer Spuren. Selbst wenn es bei den Informationen gar nicht um Ihre Firma geht, gefährden Sie Ihren Job, weil diese nicht in diesen Vorgang involviert sein will.

3. USB-Stick benutzen

Wenn Sie Daten weitergeben wollen, kopieren Sie diese auf einen USB-Stick. Am besten verschlüsseln Sie den etwa mit dem TrueCrypt-Nachfolger VeraCrypt. So ist sichergestellt, dass ohne Ihr Zutun niemand auf diese Informationen zugreifen kann. Alternativ können Sie zum Beispiel auch ein ZIP-Archiv mit einem Passwort schützen. Das können Sie etwa mit dem kostenlosen Tool 7zip erstellen. Am besten verwenden Sie dabei das 7z-Format, das anders als ZIP-Dateien auch die im Archiv enthaltenen Dateinamen verschlüsselt.

4. Auf HTTPS-URL achten

Sie können den heise Tippgeber dann später ohne großes Risiko etwa bei sich zu Hause nutzen. Achten Sie auf die exakten Schreibweise der URL https://heise.de/tipps und das grüne Schloss-Symbol. Brechen Sie bei eventuellen Zertifikatswarnungen sofort ab. Durch die https-Verschlüsselung weiß selbst jemand, der Ihre Internet-Verbindung überwacht, nicht, ob Sie gerade heise-Security-News via HTTPS lesen (das ist mittlerweile möglich) oder uns über den heise Tippgeber Informationen zuspielen.

5. Uploads verschlüsseln

Über das anonyme Kontaktformular können Sie uns nur Text, aber keine Dateien übermitteln. Bei weniger brisanten Dingen können Sie jedoch die (verschlüsselten) Daten etwa bei einem One-Click-Hoster wie transfer.sh hochladen und uns die URL und Passwort über das heise-Tippgeber-Kontaktformular übermitteln. Beachten Sie dabei jedoch, dass der Upload-Server unter Umständen Ihre IP-Adresse protokolliert. Im Zweifelsfall sollten Sie lieber unseren sicheren Briefkasten via Tor nutzen.

6. Anonym durch Tor

Die Nutzung von Tor beim Übermitteln brisanter Daten bietet mehr Anonymität. Um das mit maximalem Schutz zu kombinieren, ist unser sicherer Briefkasten für heise Tippgeber als Tor-Service realisiert. Sie erreichen ihn über den Tor-Browser, den Sie einfach herunterladen, installieren und starten.

7. Anonym am Hotspot

Selbst eine Überwachung Ihrer Internet-Verbindung zeigt damit nicht mehr als die Tatsache, dass Sie Tor benutzt haben. Auch das können Sie vermeiden, indem Sie nicht Ihr eigenes Netz, sondern ein öffentlich zugängliches benutzen, also etwa einen offenen Hotspot.

8. Rückstandsfrei durch Tails

Sie hinterlassen immer noch Spuren auf Ihrem PC. Möglicherweise bereits auf Ihrem System platzierte Überwachungs-Software kann trotz Tor-Verschlüsselung auf die brisanten Informationen zugreifen und auch protokollieren, wann und wem Sie sie übermittelt haben. Starten Sie deshalb auf dem Rechner das speziell gesicherte, garantiert saubere Live-System Tails. Es wickelt alle Internet-Verbindungen über Tor ab. Und wenn Sie den PC später neu starten, gibt es darauf keine Spuren mehr von dem, was Sie unter Tails damit gemacht haben.

9. Meta-Daten entfernen

Bleiben die Daten selbst: Es kann natürlich sein, dass diese Daten Hinweise auf Ihre Identität geben. Sie können diese zum Teil selbst entfernen, etwa mit dem in Tails enthaltenen Metadata Anonymisation Toolkit (MAT, erhältlich auch über den Link am Ende des Artikels). Wir empfehlen allerdings, dass Sie die Daten lieber im Originalzustand belassen und dem Investigativ-Team der c’t-Redaktion vertrauen, dass wir verantwortungsbewusst mit den von Ihnen gelieferten Informationen umgehen. Wir werden dabei alles uns Mögliche tun, um Ihre Identität zu schützen und Schaden von Ihnen fernzuhalten.

10. STFU

Der wichtigste Tipp für Whistleblower überhaupt: Reden Sie mit niemandem über Ihre geheimen Aktivitäten. Viele anonyme Whistleblower fliegen nicht etwa wegen verräterischer Spuren auf, sondern durch Verrat im persönlichen Umfeld. Chelsea Manning, die uns damals noch als Bradley die Augen für Kriegsverbrechen im Irak („Collateral Murder“) öffnete, sitzt heute in einem US-Gefängnis, weil sie sich dem Ex-Hacker Adrian Lamo anvertraut hatte und der die Information an US-Behörden weitergab.

Die Tools für Tippgeber: ***ct.de/y96h***

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover