Sicherheit für den Whistleblower
Soziale Risiken
Technologische Risiken
Sozialer Schutz
Technischer Schutz

Sicherheit für den Whistleblower

Bei der Übermittlung sensibler Informationen müssen Sie die Risiken berücksichtigen, die für TippgeberInnen durch die Offenlegung von Informationen über eine Drittpartei entstehen können. Ein so betroffene Drittpartei kann Vergeltungsmaßnahmen gegen Sie oder gegen SwissLeaks ergreifen.

Während des gesamten Whistleblowing-Prozesses anonym zu bleiben, ist eine gute Möglichkeit, sich selbst und andere vor externen Bedrohungen zu schützen. Dieses Dokument befasst sich mit den Gefahren, die mit der Übermittlung von Informationen an SwissLeaks verbunden sind. Ebenso wichtig sind natürlich die Möglichkeiten, diese Risiken zu minimieren.

Soziale Risiken

Während technische Methoden, um Ihre Identität zu entdecken, einschüchternd erscheinen mögen, sind die Menschen um Sie herum die grösste Bedrohung für Ihre Anonymität.

Bevor Sie Informationen einreichen, sollten Sie überlegen, was passiert, nachdem die Informationen weitergegeben wurden und was passiert, wenn das Leck öffentlich wird.

Stellen Sie sich die folgenden Fragen, um Ihr Risiko einzuschätzen:
Handeln Sie im öffentlichen Interesse oder mit boshafter Absicht?
Werden Ihre Handlungen eine gewalttätige oder juristische Reaktion einer Gruppe hervorrufen?

Haben andere Personen als Sie Zugang zu den Informationen, die Sie übermitteln werden? Wenn diese Informationen die Öffentlichkeit erreichen, wird Sie jemand danach fragen? Können Sie den Stress einer internen oder externen Untersuchung bewältigen?

Sie sollten sich erst dann Gedanken darüber machen, wie Sie die Tipps weitergeben können, wenn Sie diese Art von Fragen ernsthaft bedacht haben.

Technologische Risiken

Die Benutzung eines Computers und des Internets hinterlässt Spuren. Spuren, die auf Ihrem eigenen Computer, dem Computer des beabsichtigten Empfängers und vielen anderen Computern dazwischen hinterlassen werden können. Diese Protokolle und andere forensische Informationen könnten einen Ermittler dazu bringen, herauszufinden, wo Sie sind und wer Sie sind.

Sie können Computerspuren hinterlassen bei:

- der Recherche der einzureichenden Informationen
- der Erfassung der einzureichenden Informationen
- beim Lesen dieser Webseite
- der Übermittlung der Informationen an uns
- beim Datenaustausch mit den Empfängern Ihrer Einreichung

Mit den richtigen Werkzeugen und Kenntnissen können Sie das Risiko, digitale Spuren zu hinterlassen und Ihre Anonymität zu gefährden, minimieren.

Sozialer Schutz

Was folgt, ist ein Minimum an Massnahmen, die Sie ergreifen sollten, um sich in sozialen Situationen zu schützen.

- Bevor Sie einen Beitrag einreichen, teilen Sie Ihre Absichten mit niemandem.
- Stellen Sie sicher, dass sich keine Überwachungssysteme oder Beobachter an dem Ort befinden, an dem Sie Informationen erfassen und übermitteln.
- Versuchen Sie sicher zu sein, dass die von Ihnen übermittelten Informationen Sie nicht identifizieren, wenn jemand anderes als der beabsichtigte Empfänger Zugang zu ihnen erhält.
- Nachdem Sie eine Einreichung gemacht haben, erzählen sie niemandem davon.
- Nachdem die Nachrichten über die Einreichung an die Öffentlichkeit gelangt sind, seien Sie vorsichtig, wenn Sie Ihre Meinung über die Nachrichten mit jemandem teilen.

Technischer Schutz

Aufgrund der technischen Komplexität moderner Computer- und Netzwerksysteme ist es anspruchsvoll, sich selbst zu schützen. Es ist möglich, aber es ist kompliziert. Sie sollten auch verstehen, dass niemand jedes Detail von Computer- und Netzwerksystemen versteht.

Wenn Sie jedoch die folgenden Richtlinien strikt befolgen, sollten Sie hinreichend sicher sein.

- Achten Sie bei der Erfassung der zu übermittelnden Informationen darauf, dass keine Spuren auf den IT-Systemen zurückbleiben, die sie identifizieren können (z.B.: Dateien mit einem USB-Stick sammeln). Wenn Sie die Einreichung abgeschlossen haben, zerstören und entsorgen Sie den USB-Stick.
- Sie sollten wissen, dass das "Löschen einer Datei" auf fast allen Computern die Spuren des Vorhandenseins der Dateien nicht von diesem Computer entfernt.
- Beachten Sie, dass Metadaten in einigen der von Ihnen übermittelten Daten enthalten sein können.
- Erwägen Sie, die Metadaten mit einem dafür geeigneten Tool zu entfernen.
- Wir empfehlen, alle Daten, die Sie uns senden, in ein Standardformat wie PDF zu konvertieren.
- Informationen müssen zwingend mit dem anonymen Tor-Browser übermittelt werden
- Bewahren Sie keine Kopien der von Ihnen übermittelten Informationen auf.
- Senden Sie keine Informationen von dem Computer, der Ihnen von Ihrem Arbeitgeber zur Verfügung gestellt wird (verwenden Sie einen anderen Computer).
- Halten Sie die Quittung, die Sie erhalten, geheim und vernichten Sie sie, sobald Sie sie nicht mehr benötigen.
- Suchen Sie nicht in den Suchmaschinen oder auf der Newsseiten nach den von Ihnen eingereichten Informationen.

Sicher genug bedeutet nicht, dass Ihre Anonymität gewährleistet ist. Es bedeutet, dass selbst Computerexperten nachträglich nicht in der Lage sein sollten, festzustellen, dass Sie die Quelle des Lecks waren.

Wenn Sie besser verstehen möchten, wie Sie in dieser digitalen Umgebung sicher vorgehen können, lesen Sie die Anleitungen, die im Rahmen des Projekts Security in a Box erstellt wurden.