Tipps zum digitalen Informantenschutz

Nicht nur die NSA und der BND lesen gern mal mit, was alles so in den E-Mails steht, die an Journalisten verschickt werden. Und in Bundesministerien ist sogar schon das eine oder andere Mal mitgeschnitten worden, was Journalisten sich so auf der hauseigenen Website anschauen. Außerdem liefert noch das Smartphone Bewegungsprofile, die Detektiven und Schlapphüten den Weg zum Informanten weisen. Dagegen hilft nur eines: Eine digitale Tarnkappe.

Von Peter Welchering

Den Wettlauf um die Identität des Informanten konnten die Reporter des Deutschlandfunks 2006 nur ganz knapp zu ihren und des Whistleblowers Gunsten entscheiden. Ein Insider aus dem Bundesministerium des Inneren hatte den Computerjournalisten Unterlagen über Planspiele übermittelt, die biometrischen Daten für den elektronischen Personalausweis an interessierte Unternehmen weiterzuverkaufen. Die Planspiele wurden nach der Veröffentlichung sofort eingestellt. Der Weiterverkauf biometrischer Daten der Bundesbürger war geplatzt.

Aber die Hatz auf den Informanten begann. Internet-Adressen-Rückverfolgung, Auswertung von Dienstmail sowie Analyse von Profildaten aus dem Kommunikationsverhalten im Internet und im Mobilfunk gehörten zu den Methoden, mit denen Netzdetektive den Insider dingfest machen wollten. Sie hatten keinen Erfolg. Denn die Reporter verschleierten jeden Kontakt mit dem Informanten mit Krypto-Chats nachhaltig, verschlüsselten alle Daten, benutzten Einmal-Browser und anonyme Telefonnummern, mailten nur über Anonymisierungsnetzwerke und surften unerkannt im Netz.

Die Netzdetektive waren zwar hochgerüstet, aber die Reporter waren ausreichend vorsichtig und beherzigten die Grundregeln für den Schutz von Informanten im digitalen Zeitalter: Möglichst wenig Spuren hinterlassen, am besten keine verwertbaren.

Externe Datenträger bieten Schutz

Dateien zu verschlüsseln, zum Beispiel mit der kostenlosen Software Locknote von Steganos, ist da ein guter erster Schritt (http://www.steganos.com/de/produkte/gratis-fuer-sie/locknote/pressestimmen/?0=). Komfortabler wird die Verschlüsselung auf der Festplatte oder dem Stick mit kommerziellen Verschlüsselungsprogrammen. Die kosten meist ab 20 Euro aufwärts, bieten aber auch ausreichend lange Schlüssel, so dass das Passwort-Cracking auch für die Profis mit Schlapphut und Superrechner zumindest höheren Aufwand bedeutet.

Ganz sensible Daten mit brisanten Informationen, die einen Informanten identifizieren können, sollten aber auch verschlüsselt nicht über Nacht einfach auf dem Büro-PC gespeichert bleiben. So etwas trägt der datenschutzbewusste Journalist auf einem externen Datenträger lieber bei sich oder schließt es im Tresor seiner Bank ein. (Als Freeware für die Verschlüsselung externer Festplatten zu empfehlen: http://www.protectcom.de/crypditor/de/) Das senkt übrigens auch die Einbruchquote in Redaktionsbüros.

Mail sollte nicht in jedem Fall lesbar sein, also muss auch hier Verschlüsselung her. Wer Freude am Installieren von Software hat, nutzt die Mail-Software Thunderbird (http://www.mozilla.org/de/thunderbird/features/), die wie der Firefox-Browser von der Mozilla Foundation herausgegeben wird. Auf der Add-On-Seite zu Thunderbird

(https://addons.mozilla.org/de/thunderbird/addon/enigmail/?src=hp-dl-featured) gibt es eine Erweiterung zum verschlüsseln von Mails und Anhängen namens Enigmail.

Mail-Verschlüsselung muss nicht schwierig sein

Diese Erweiterung setzt allerdings die Verschlüsselungsroutine Gnupg (www.gnupg.org) voraus. PGP und Verwandtes bieten zwar eine gründliche Verschlüsselungslösung und die Möglichkeit, ohne Passwort-Versand zu kryptieren. Allerdings ist eine solche asymmetrische Verschlüsselung leider nur mit einigem Aufwand zu installieren.

Wem das zu mühsam ist, kann seine Botschaft einfach in eine Datei schreiben, mit einem Verschlüsselungsprogramm unlesbar für Dritte machen und als Mail-Anhang auf die Reise schicken. Zum Beispiel beim Crypditor ist auch das Entschlüsselungsprogramm gleich mit im Mailversand enthalten.

Der Empfänger benötigt dann nur noch das Passwort zum Entschlüsseln. Das sollte zumindest mit separater Mail, besser auf einer Postkarte verschickt werden. Der frühere Leiter der Cybercrime Unit von Interpol hat auf einer Verfassungsschützertagung in einem halbstündigen Vortrag ausgeführt, warum Postkarten die Schlapphüte nicht interessieren und nicht analysiert werden müssen. Das bietet eine Chance für den Passwort-Versand und die Verabredung von vertraulichen Treffen.

Anonymisierungsserver sind unerlässlich

Mit Verschlüsselung ist übrigens noch keine Anonymität erreicht. Durch die mitgelieferte Internet-Protokoll-Adresse kann die Mail zurückverfolgt werden. Eine Lösung bieten hier Anonymisierungsserver, wie www.anonymouse.org, die allerdings nicht immer ganz verlässlich arbeiten. Zum anonymen Surfen sind sie gut geeignet. Beim Mailversand ist jedoch die Quote der verschwundenen Mails zu hoch.

Recht zuverlässig dagegen arbeitet das Anonymisierungsnetzwerk TOR. Das Kürzel steht dabei für „The Onion Router“, weil die Datenpäckchen, zum Beispiel einer Mail, wie bei einer Zwiebel immer eine Schickt mehr übergezogen bekommen, je mehr Server einbezogen werden. (https://www.torproject.org. Doch die Installation der notwendigen Software auf dem eigenen PC ist nicht ganz trivial.

Besser arbeiten lässt sich da mit verschlüsselten Dateien und toten elektronischen Briefkästen. Dazu benötigen Informand und Informant nur ein Benutzerkonto bei einem Cloud-Anbieter. Das kann sogar die Dropbox sein. Ihre Miteilungen verschlüsseln sie, laden die verschlüsselte Datei in die Cloud und nutzen dafür stets einen Anonymisierungsserver wie anonymouse.

Tote Briefkästen gibt es auch digital

Die Nachrichten werden entweder zu festgelegten Zeiten ausgetauscht, oder nach dem Upload erhält der Empfänger eine zuvor abgesprochene harmlose Mail, eine Postkarte, einen Anruf oder eine Direktmitteilung via Twitter. Er weiß dann, dass der tote Briefkasten bestückt ist und er sich eine Mitteilung herunterladen kann.

Damit die mit Programmen wie Word, Excel oder einem beliebigen Editor erstellten und sofort verschlüsselten Dateien nicht aus dem PC-Datenmüll rekonstruiert werden können, müssen die von fast allen Softwarepaketen angelegten temporären Dateien gesucht und

gelöscht werden. Eigentlich sollte jede Anwendung die von ihr erzeugten temporären Dateien gleich mit der Beendigung des Programms löschen.

Doch in vielen Fällen geht das schief, und so können Dokumente aus den Dateien mit der Kennung „tmp“ rekonstruiert werden. Da hilft nur eines: wirksam löschen. Macht man das nur mit dem Dateimanager und dem „Entfernen-Befehl“, bleibt die Datei dort liegen, wo sie physikalisch abgespeichert wurde. Nur ihr Eintrag in der Dateitabelle wird gelöscht. Damit ist sie dann für das Betriebssystem nicht mehr auffindbar, aber sehr wohl noch für die forensischen Programme von Netzdetektiven.

Die eigene Festplatte ist ein Risiko

Denn die eigentlich gespeicherten Bits, also die Abfolge von Nullen und Einsen, bleiben solange auf der Festplatte liegen, bis der Speicherplatz wieder gebraucht wird. Erst dann werden sie überschrieben. Da kann es durchaus passieren, dass sie noch viele Tage bis Wochen, nachdem der „Delete-Befehl“ erfolgt ist, als physische Information noch verfügbar sind.

Hier hilft aber das kleine Programme „Erase“, auch als Open-Source-Software verfügbar (http://eraser.heidi.ie/). Erase überschreibt die zu löschenden Dateien mit einer Bitfolge, und das dreimal, viermal oder siebenmal, je nachdem, welches Sicherheitsbedürfnis der Festplatteneigner hat.

Ganz wichtig ist es auch, bei Treffen mit Informanten kein Handy mitzunehmen oder zumindest den Akku herauszunehmen. Letzteres ist beim iPhone ja nicht so ohne weiteres machbar. Aber es ist notwendig. Denn auch ein ausgeschaltetes Handy kann von digitalen Spionen über den Kontrollkanal eingeschaltet und als Wanze benutzt werden. So können Gespräche einfach belauscht oder bei Smartphones mit Kamera sogar erstklassige Videoaufnahmen von den Ausspionierten angefertigt werden.

Chatten ist oft sicherer als Telefonieren

Telefonieren ist ohnehin eine gefährliche Sache. Mit Informanten sollte man tunlichst weder über das Festnetz noch via Mobilfunk sprechen. Zum Erstkontakt ist allerdings oftmals eine Telefonnummer unerlässlich. Die aber sollte dann anonym sein. Sogenannte „nicknumbers“ helfen da weiter (http://web.nicknumber.de/faq.php). Je nach Anbieter kostet eine solche anonyme Anrufnummer, die auf das eigene Telefon oder einen Web-Sprachdienst weiterschaltet, zwischen 10,00 und 30,00 Euro für die Einrichtung der Nummer sowie monatliche Grundgebühren von 3 Euro bis 15 Euro. Auch anonym gekaufte Prepaid-Karten fürs Mobilfunknetz und ein nur für diesen Zweck ebenso anonym beschafftes und natürlich bar bezahltes Handy leisten hier gute Dienste. Aber dieses Handy darf dann wirklich nur für die Kommunikation mit dem Informanten genutzt werden. Im Alltag ist das Gerät absolut Tabu!

Eine Alternative zum Telefonieren bietet der Chat. Hier kommt es wesentlich auf die Chat-Software an. Pidgin beispielsweise erlaubt verschlüsseltes Chatten in rund 15 Chat-Netzwerken vom Instant Messaging Service von AOL bis hin zu Yahoo (http://www.pidgin.im/). Mit dem Plugin TorChat für die Anonymisierung der Verbindung und https://github.com/prof7bit/TorChat/downloads und dem Verschlüsselungs-Plug-in „Off-the-Record-Messaging“ (http://www.cypherpunks.ca/otr/) ist dann nur unter sehr großem Aufwand das Abhören des Chats möglich.

Wer zudem bei sehr sensiblen Netz-Nutzungen nicht vom eigenen PC aus agiert, sondern in ein Internet-Cafe geht, bei dem er sich nicht ausweisen und anmelden muss und in dessen Umgebung auch keine Kameras für die Videoüberwachung installiert, hat den Informantenschutz auch im digitalen Zeitalter ernst genommen.

Ohnehin: die Überwachungskameras im öffentlichen Raum erschweren unseren investigativen Job ganz massiv. Im oben erwähnten Fall der Recherche zum Weiterverkauf biometrischer Daten der deutschen Personalausweisinhaber haben die Reporter vor jedem Treff mit dem Informanten erheblich viel Zeit in die Ermittlung kamerafreier Routen und Treffpunkte investiert.