COMPUTER

Verborgenes Tattoo

Das Internet verhilft einer uralten Technik zu neuer Blüte: der Steganografie. Mit ihr lassen sich geheime Botschaften in Fotos, Musik oder Videos verstecken.

Histiaios, Tyrann von Milet im antiken Kleinasien, erwies sich als besonders listiger Revoluzzer: Den Aufruf zum Aufstand gegen die persischen Machthaber ließ er einem Sklaven in die Schädelhaut tätowieren, dann wartete er, bis das Haar nachgewachsen war.

Dann schickte er den Mann in die besetzte Stadt. Nicht einmal der Bote selbst wusste, welchen Text er unter der Tolle trug, bis der Adressat – Schwiegersohn des Tyrannen – ihm am Ziel den Kopf wieder scheren ließ.

Histiaios war gewiss nicht der erste Trickser, der eine Botschaft nicht verschlüsselte, sondern schlicht versteckte – die sogenannte Steganografie gilt als uralte Finte der Menschheit. Man benutzte Wachstafeln, Geheimtinte, doppelte Böden. Heute bietet die digitale Welt deutlich ausgefuchstere Verstecke.

So bediente sich Anna Chapman, die rotschopfige Russin, der moderneren Möglichkeiten der Steganografie. Die schöne Spionin, die 2010 in den USA aufflog, versteckte ihre Botschaften unter anderem in den Pixeln von Fotos, die sie öffentlich im Internet postete. Aber nur Eingeweihte konnten sie lesen.

Oder der kolumbianische Drogenboss Juan Carlos Ramírez Abadía: Nach seiner Verhaftung vor sechs Jahren stellte sich heraus, dass er seine Kassiber gern in Abbildungen der japanischen Kultfigur Hello Kitty verborgen hatte. Das niedliche Kätzchen half ihm, Kokainlieferungen zu koordinieren.

Agenten, Mafiosi, Terroristen – lange schien die Steganografie sich vor allem für verbrecherische Umtriebe zu eignen. Aber mit den Enthüllungen um die Internetüberwachung durch Geheimdienste wie die amerikanische NSA erobert das digitale Versteckspiel nun langsam den bürgerlichen Alltag.

Steganografie verlockt, allein schon, weil Hello-Kitty-Bilder oder lustige Privatfotos so unglaublich unverdächtig sind. Wer hingegen seine Nachrichten mit ausgefeilten Systemen wie „Tor“ oder „PGP“ verschlüsselt, der muss etwas zu verbergen haben, oder?

Zuletzt wurde Steganografie vor allem dazu verwendet, Musik, Fotos oder E-Books heimlich zu markieren. Verleger prägten den Werken ein digitales Wasserzeichen ein; so lässt sich verfolgen, wer die Dateien illegalerweise in Tauschbörsen feilbietet.

Mittlerweile jedoch gibt es jede Menge Steganografie-Programme für jedermann, herunterzuladen im Internet. Einige sind kinderleicht zu bedienen, so wie die Android-Software „Pixelknot“: Foto machen, Software öffnen, Geheimcode eintippen, Passwort vergeben, Bild verschicken. Der Empfänger öffnet das Foto ebenfalls mit „Pixelknot“, gibt das Passwort ein und liest die geheime Botschaft.

Ob Foto, Musik oder Video – prinzipiell lässt sich in jeder Datei Vertrauliches so klandestin verstauen wie der antike Appell im Schädeltattoo. Sogar der Internetbrowser Firefox kann versteckte Depeschen verschicken; dafür muss man nur das kleine Zusatzprogramm „Simple Steganography“ installieren, entwickelt von der deutschen Programmiererin Corinna John.

Allerdings wächst mit der Raffinesse der digitalen Schlupflöcher die Fähigkeit, diese zu enttarnen. So lassen sich inzwischen selbst kleinste Veränderungen von Bilddateien aufspüren. Wer also unbemerkt bleiben will, raten Experten, sollte die vertraulichen Infos möglichst knapp fassen; sie dürfen nicht mehr als ein Prozent der gesamten Tarndatei ausmachen.

„Die meisten Stego-Programme sind Scharlatanerie“, warnt auch Jessica Fridrich von der Binghampton University im US-Bundesstaat New York, eine der führenden Expertinnen auf dem Gebiet. Anbieter wie beispielsweise Booz Allen Hamilton, die Firmen vor Cyber-Attacken schützen, verfügten bereits über ausgefeilte Analyseprogramme, die gezielt nach verborgenen Botschaften suchen. Fridrich selbst hat zum Knacken jenes Codes beigetragen, den auch „Pixelknot“ verwendet.

„Software wie ‚Pixelknot‘ ist nur ein Spielzeug“, sagt Krzysztof Szczypiorski, Professor für Telekommunikation an der Technischen Universität Warschau. „Steganografie ist ein Katz-und-Maus-Spiel.“

Er muss es wissen, sein Team testet, wie die Maus der Katze entkommen könnte. Etwa mit dem „Hiccups“-System: Es versteckt Botschaften in Datenpaketen, die vermeintlich bei der Übertragung beschädigt worden sind. Noch eleganter ist die Methode „Skype Hide“. Sie bettet Botschaften in die Redepausen von Videokonferenzen ein. Der Adressat liest dabei, wörtlich, zwischen den Zeilen.

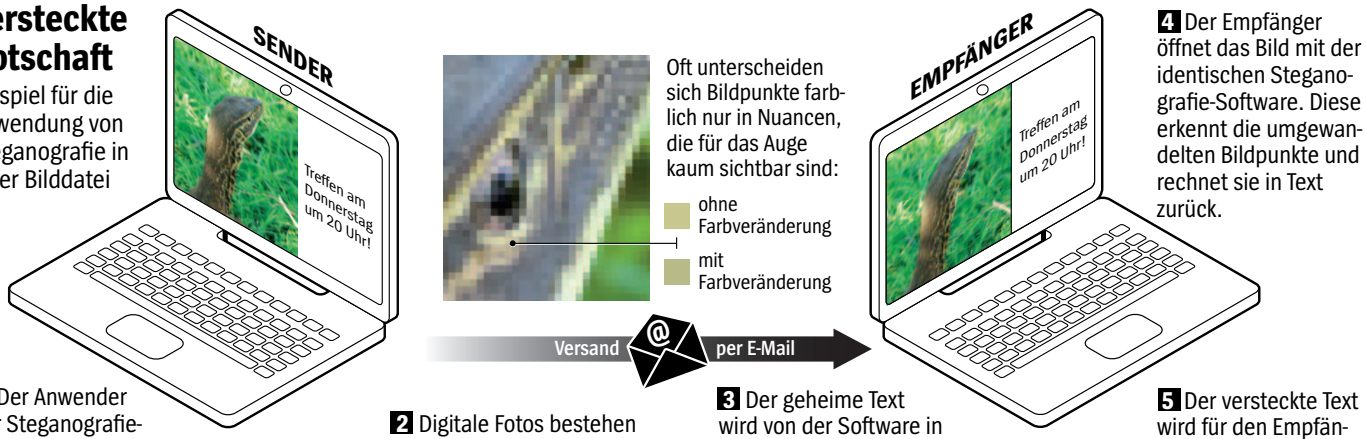
Bis zu zwei Kilobit pro Sekunde lassen sich mit „Skype Hide“ heimlich übertragen, weitaus effizienter als in einem Hello-Kitty-Bild. Hier ergibt sich ein neuer Sinn des alten Bonmots von Cicero: Cum tacent, clamant – indem sie schweigen, rufen sie.

Dass er mit seiner Arbeit Werkzeuge für Kriminelle herstellt, lässt Szczypiorski nicht gelten: „Steganografie ist wie ein Messer, mit dem man Brot schneiden oder morden kann“, sagt er. „Wir bekommen auch viele Anfragen von Dissidenten aus Diktaturen mit scharfer Zensur.“

Hilmar Schmundt

Versteckte Botschaft

Beispiel für die Anwendung von Steganografie in einer Bilddatei



1 Der Anwender der Steganografie-Software ruft ein beliebiges Bild auf und gibt einen Text ein, der verschlüsselt werden soll.

2 Digitale Fotos bestehen aus unzähligen Bildpunkten, die jeweils eine bestimmte Farbinformation beinhalten.

3 Der geheime Text wird von der Software in kleinste Farbveränderungen einzelner Bildpunkte umgerechnet und dann verschickt.

4 Der Empfänger öffnet das Bild mit der identischen Steganografie-Software. Diese erkennt die umgewandelten Bildpunkte und rechnet sie in Text zurück.

5 Der versteckte Text wird für den Empfänger wieder sichtbar.

DER SPIEGEL