# Gottes vergessene Kinder - Steganographie und alternative Datenströme

"Wenn der IT-Sicherheitsbeauftragte in der Kantine nicht mehr gegrüßt wird, dann macht er seinen Job richtig!" oder dagegen: "Funktionalität geht vor Sicherheit!" - nichts ist so schwer durchzusetzen, wie ein gutes Sicherheitskonzept in der EDV. Hoffnungsvoll investieren Geschäftsführer in teure Programme, die die Sicherheit im Unternehmen garantieren sollen und scheitern, weil sich ihre Mitarbeiter geschickt um die gemachten Vorgaben herummogeln und ihre wichtigen Daten doch unverschlüsselt auf dem Laptop ins Ausland transportieren. Dabei muss Datensicherheit nicht teuer sein, man muss sie nur akzeptieren und kann dann mit einfachen Mitteln viel bewirken.

## Aperta transire - Am Offensichtlichen vorübergehen

Wer Daten verbergen will, muss sich einer menschlichen Eigenheit bedienen, die schon seit Kindheitstagen bekannt ist: Je größer der Spickzettel, desto weniger entdeckt ihn der Lehrer. Auf EDV-Deutsch bedeutet dies: je deutlicher versucht wird, etwas zu verschlüsseln, mit Passwörtern zu sichern oder mit Berechtigungen zu belegen, desto neugieriger werden die Angreifer und umso ausgefeilter ihre Methoden. Es setzt sich eine Spirale in Gang, bei der Mal der Verschlüsselungsexperte, mal der Hacker die Nase vorn hat. Aber für die 5000 Urlaubsbilder (alle Sonnenuntergänge 2001-2010) und die 6GB an mp3-Dateien (Gesamtwerk Georg Philipp Telemann) interessieren sich nur Musikfreunde und Fotofanatiker. So erregt auch eine verschlüsselte Email größere Aufmerksamkeit als 5 lustige Bilder von tobenden Katzen. Dieses Verhalten ist schon seit dem Altertum bekannt und findet in verschiedenen Techniken ihren Niederschlag.

## Du hast den Farbfilm vergessen… Steganografie

Wenn also lustige oder langweilige Bilder für Hacker und Spione nicht interessant sind, warum nicht wichtige Daten darin verstecken. Was kompliziert klingt und mit dem Namen Steganographie nicht gerade der modernen IT-Nomenklatur entspricht, kann ganz einfach sein: im Internet sind zahlreiche kostenlose oder zumindest günstige Programme erhältlich, die es einem ermöglichen, Daten hinter Bildern oder Musikdateien zu verstecken (vgl. www.datenschutzzentrum.de). Ziel des Verfahrens ist, Daten so hinter ein Bild oder Musikstück zu legen, dass einem Dritten beim Betrachten des Offensichtlichen nichts auffällt. Um ganz sicher zu gehen, können wichtige Daten zuerst verschlüsselt und dann passwortgeschützt versteckt werden. Dabei sind Bilddateien unempfindlicher als Audiodateien.

## Die Technik

Bei der digitalen Steganographie werden die Farbinformationen leicht modifiziert und Bits verändert, ohne dass es dem menschlichen Auge auffällt. Bilder mit einer hohen Pixelzahl eigenen sich daher besser, denn es sind viel mehr Farbinformationen enthalten, als man sehen kann. Jeder Pixel zeichnet sich durch drei Farbwerte aus, rot, grün und blau, die jeweils einen Wert zwischen 0 und 255 haben. Alle diese Werte können unmerklich verändert werden und so ist es möglich in einem Bild 640x480 Pixel eine Datenmenge von rund 112 Kilobyte zu verstecken. Je mehr Farbwechsel ein Bild hat, desto mehr Daten können dahinter verschwinden.

## Tipps und Tricks

Die Steganographie-Programme sind oft sehr klein und einige müssen nicht auf der Festplatte installiert werden. Es empfiehlt sich also folgende (paranoide) Vorgehensweise:

Besorgen Sie sich ein Steganographie-Programm, das nicht installiert werden muss (z.B. JPHS for Windows) und teilen sie das Ihrem Gegenüber persönlich an einem abhörsicheren Ort mit, z.B. beim Joggen im Wald.
Laden Sie das Programm aus dem Internet auf einen USB-Stick herunter, möglichst über einen PC auf dem Sie nicht identifiziert werden können (Internet-Cafe). Suchen Sie sich dann schöne Bilder Ihres Urlaubs und hinterlegen Sie sie mit dem geheimen Text (Programm nicht auf dem eigenen PC speichern!), verpassen der Datei ein Passwort (per SMS an das Gegenüber) und verschicken Sie sie mit einem netten Text per Email. Das war es.
Es ist aber darauf zu achten, dass die Bilder nach dem Stenografieren nicht bearbeitet und konvertiert werden. In diesem Fall gehen die Daten der versteckten Datei verloren.

## Bewegte Bilder

Müssen Daten in Echtzeit geschützt übertragen werden, eigenen sich auch Videokonferenzen, um Daten versteckt zu übertragen. Bei einer Videoübertragung werden zwar durch verlustbehaftete Kompressionsverfahren die Datenmengen verringert, doch ist es möglich mit Hilfe von in die Kamera eingebauten steganographischen Systemen, Daten zu verstecken. In diesem Fall wird, aufgrund des Übertragungsverfahrens, eine andere Technik angewendet: Bei der Übertragung wird das Bild zeilenweise aufgebaut und die Bildpunkte haben in vertikaler Ausrichtung ein festes Raster, nur horizontal sind sie frei. Hier setzt die Steganograpie ein und verändert die horizontalen Werte. Faktisch entsteht ein neues Bild, das übertragen wird, doch da das unveränderte Originalbild nicht mitgeschickt wird, ist die versteckte Datenübermittlung für einen Angreifer nicht zu bemerken.

## Steganographie und Urheberrechte

Da Steganographie kein Verschlüsselungsverfahren ist und technisch auch nicht so behandelt wird, kann die Steganographie durchaus in Bereichen eingesetzt werden, in denen Verschlüsselung verboten ist.
Ein weiteres Anwendungsgebiet der Steganographie findet sich im Bereich des Urheberrechts und des Copyrights. Bilder, Musikstücke oder Videos können mittels Steganographie gekennzeichnet werden. Die Datei kann nun kopiert und verschiedenen Personen zugesendet werden. Sobald die Datei bearbeitet wird, lässt sich das hinterlegte Copyright nicht mehr anzeigen. Ein Vergleich mit der gesicherten Originaldatei beweist somit eine Manipulation.
Mit Hilfe des Watermarking, können Daten des Käufers in ein Objekt steganographisch eingebettet werden (Fingerprinting) und so kann vor Gericht die illegale Weitergabe der Daten nachgewiesen werden.

## Dateien verstecken für Geübte

Wie mittels ADS unter Windows Daten versteckt und aufgespürt werden können, erfahren Sie in „Gottes vergessene Kinder – Teil 2: Alternative Datenströme“