STEGANOGRAPHIE
2015/02/01

Was ist **Steganographie?** Es bedeutet soviel wie: „Verstecktes Schreiben“ oder „Geheimes Schreiben“. Dabei wird die Möglichkeit genutzt in einer unscheinbaren Nachricht eine wichtige oder geheime Information zu verstecken, die nur vom Empfänger entschlüsselt werden kann. Alle, die die Nachricht ansonsten lesen, können die mitgeführte Information nicht wahrnehmen. Sie sehen oder lesen nur eine unauffällige Information ohne weiteren Wert.

Als Beispiel nehmen wir mal dieses total alte Online-Werkzeug:

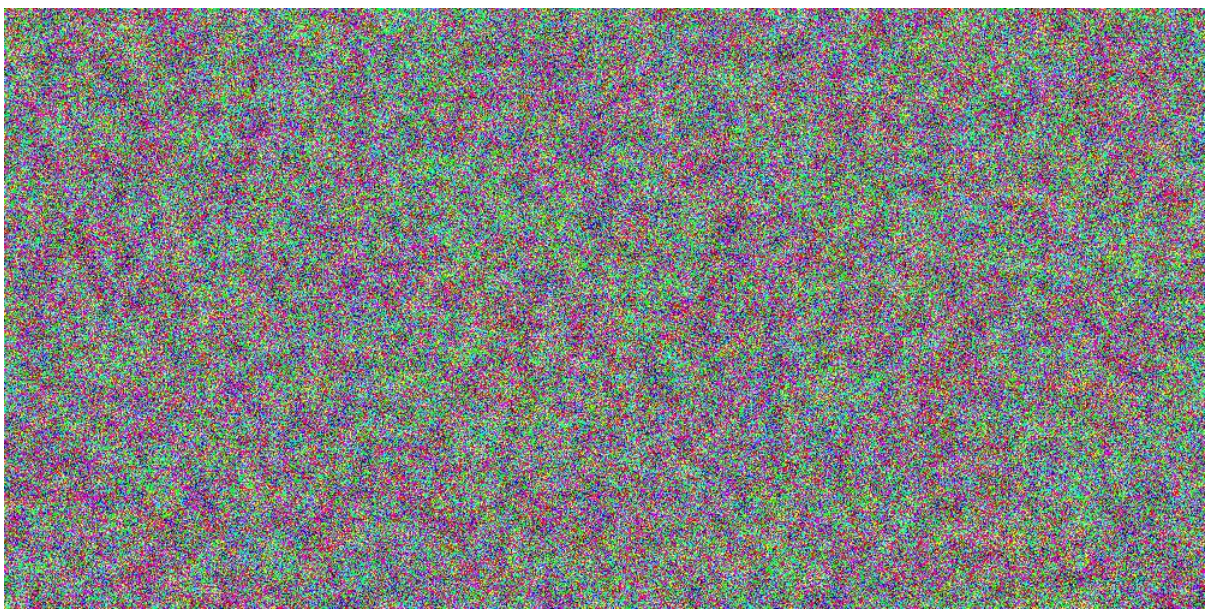
Was versteckt sich hier:

The card strongly places to the powerful structure. I move idle yogis near the lazy wet bathroom. Sometimes, trees lean behind tall skys, unless they’re clear. Never play mercilessly while you’re selling through a ugly frame. We eerily open around quiet opaque highways. While dogs stupidly restrain, the units.

Richtig: Nachdem Ihr Copy & Paste gemacht habt – *also die Fähigkeit besitzt einen Dr.-Titel zu erwerben* – könnt Ihr die Nachricht nach einem Klick auf *decode* laut vorlesen: **Ich liebe kowabit.de!**

Mit unseren technischen Möglichkeiten können wir geheime oder wichtige Dateien bzw. Informationen mit so gut wie jeder anderen Datei transportieren. Grundsätzlich bieten sich Audiodateien, Textdokumente, Videodateien, meist Bilddateien an. Diese Trägerdateien können normale bis unwichtige Informationen beinhalten. Werden Kriminelle, Geheimdienste oder andere Institutionen auf diese Daten aufmerksam, können sie, außer bsp. Urlaubsbilder, kaum etwas entdecken. In diesen unscheinbaren Informationen sind jedoch geheime Daten versteckt. Bei der Masse an Informationen die mittlerweile auf normalen HeimPCs zu finden sind, ist es so gut wie ausgeschlossen, dass interessierte Augen die versteckten Informationen entdecken, wenn Nutzer ein umsichtiges Anwendungskonzept umsetzen.

Das lässt sich bspw. durch das Verstecken einer Information in Einem unter vielen Bildern erledigen. Hier kann man das Werkzeug OpenPuff nutzen. Es versteckt nicht nur Informationen in anderen Informationen, sondern verschlüsselt die geheime Info auch noch. Sogar ein Aufteilen auf mehrere Trägerdateien ist möglich. Wenn Ihr mit diesem Werkzeug das folgende Bild mit den Passwörtern (A, B, C):
PostvonFreunden diekeinerbraucht umglücklichzusein entschlüsselt und entpackt, könnt Ihr eine von Anonymous-Hackern im Dezember 2014 veröffentlichte Information erhalten (*,deren Wahrheitsgehalt nicht wirklich sicher ist.*):



In OpenPuff kippt Ihr zum Enttarnen der geheimen Info einfach die Bilddatei rein und nutzt die oben angegebenen drei Passwörter.

Übrigens kann man die drei Passwörter auch auf drei Personen aufteilen, um die Entschlüsselung nur unter sechs Augen zu ermöglichen. Nach dem Prinzip arbeitet bspw. auch das Werkzeug Secret Sharp. Außerdem bietet sich das Werkzeug DeepSound an, um Infos in Sounddateien einzugraben. Als Alternative könnt Ihr mit Camouflage Daten in ein JPEG stecken. Einfach mal ausprobieren.

Wer **kowabit.de** aufmerksam nutzt, weiß, dass ich Steganographie-Fan bin und diese Form der Datentarnung empfehle, um wichtige Infos zu transportieren. Das hat auch mit den Erkennungsmöglichkeiten zu tun und den Anwendungsstrategien.

Eine Verschlüsselte E-Mail wird erkannt. Sie kann nur nicht gelesen werden. Grundsätzlich kann man aber davon ausgehen, dass man jetzt *interessant* für gewisse Kreise ist. Mit harmlosem Urlaubsbilderaustausch oder dem Tauschen von Sounddateien fällt man in der Masse der Nutzer nicht auf. Natürlich kann man auch diese Nachrichten dann verschlüsseln. Sollte mal jemand nach dem Schlüssel fragen, wäre es relativ ungefährlich die Schlüssel rauszugeben. Es sind ja nur private E-Mails mit normalem Inhalt. Und Verschlüsseln tun wir alle nur, um unsere persönlichen Daten zu schützen.

Steganographie kann aber mit statistischen Berechnungen enttarnt werden. Durch die Verschlüsselung getarnter Daten selbst, ist aber mittlerweile auch das nach meiner Meinung kaum von Bedeutung. Auch digitale Kameras und selbst Grafikprogramme werfen mittlerweile Bilder aus, die sehr wenig Platz für Steganographie bieten. Deshalb ist hier bereits eine statistische Berechnung nur schwer durchzuführen. Gescannte Bilder bieten oft mehr Platz.
Desweiteren ist Steganographie erfahrungsgemäß sehr schwach verbreitet, weshalb automatisierte Verfahren zur Analyse von Bilddateien (o.a.) eher kaum existieren. Alles nur ein weiteres Rauschen in einer Fülle von Daten.
Eine weitere Enttarnungsmöglichkeit ist bspw. zusätzlich die falsche Anwendung von Steganographie. Wenn die Trägerdatei oder die Trägerdateien zu wenig freien Platz bieten, oder vielleicht sogar viel kleiner sind als die zu versteckende Information, kommen verdächtige Dateien heraus. Wer also ein Video mit 10MB in ein 100KB-Bild steckt, erhält ein 10MB+ Bild. Das wäre dann verdächtig. Software wie OpenPuff gibt dem Nutzer aber einen entsprechenden Hinweis.

Eigentlich kann man nichts mehr falsch machen. Ihr müsst Euch nur merken welche Trägerdateien welche Daten enthalten und Ihr solltet einen sicheren Passwortaustausch umsetzen.