

Operation Heiße Luft

Ein Artikel von mir auf [Telepolis](#), 31.12.2007: „Operation Heiße Luft“ – „Der angeblich „riesige Kinderporno-Skandal“ unter dem Code-Namen „Operation Himmel“ hat sich als Operation Heiße Luft erwiesen. Das Reizwort „Kinderpornografie“ verführt deutsche Medien häufig zu einer kruden Mixtur aus Halbwahrheiten, urbanen Märchen und glatten Falschmeldungen“. [\[mehr...\]](#)

24C3: Die Zukunft von Tor und anderer Anonymisierungsdienste

[Heise Newsticker](#): 24C3: „Die Zukunft von Tor und anderen Anonymisierungsdiensten“

(...) „Einen neuen Seitenhieb auf die besonderen Schwierigkeiten, die allein deutsche Strafverfolger den Betreibern von Tor-Servern immer wieder bereiten, konnte sich Dingledine nicht verkneifen. Es sei nötig, den hiesigen Ermittlern besser zu erläutern, „wie das Internet funktioniert“ und dass es darin zahlreiche Gefährdungen für die Privatsphäre gebe. Er werde kommende Woche persönlich mit Fahndern in Baden-Württemberg sprechen und bemühe sich um weitere Kontakte zu Strafverfolgern hierzulande. Nötig sei es auch, Rechtsanwälte speziell auf die Besonderheiten des Anonymisierungsnetzes hinzuweisen und eine juristische FAQ-Liste zu erstellen.“ (...)

Übrigens nimmt nicht nur der CCC Spenden für derlei Zwecke und

für die Aufrechterhaltung deutscher Server entgegen, sodass sie auch hierzulande von der Steuer abzusetzen seien“, sondern auch die German Privacy Foundation ([GPF](#)) Der Autor hätte das wissen müssen, denn er hat über uns schon [berichtet](#).

By the way: Heise benutzt einen falschen Genetiv in der Überschrift. Es muss heißen: „Die Zukunft von Tor und (die) anderer Anonymisierungsdienste“.

24C3 | Big boobs bei den Jugendschutzwarten!



The screenshot shows a web browser window with the address bar containing 'http://www.jugendschutz.net'. The browser's menu bar includes 'Datei', 'Bearbeiten', 'Ansicht', 'Chronik', 'Lesezeichen', 'Extras', and 'Hilfe'. The browser's toolbar shows 'Zurück', 'Vor', 'Neu laden', 'Stopp', 'Drucken', 'Neuer Tab', 'Startseite', and a dropdown menu set to 'None'. The website 'jugendschutz.net' is displayed, with a search bar containing 'Ergebnisse der Suche' and a search button. The search results show 'Ergebnisse Ihrer Suche nach "\\>'" and a large image of a woman lying on a dark sofa, wearing black lingerie and high heels. Below the image, the text reads 'Suchergebnisse Website' and 'Es wurden keine zu Ihrer Suche passenden Dokumente gefunden.'

[Auch hier](#) die Hacks angucken! Die Dame ist übrigens [Vida Guerra](#).

August Hanning | Annette Ramelsberger

Im [Wikipedia](#) Artikel über Staatssekretär August Hanning fiel mir ein Link auf: „Annette Ramelsberger: Deckname Offenheit. In: [Süddeutsche Zeitung](#). 6. Oktober 2004.“ Das betreffende Elaborat ist ein völlig unkritischer Jubel-Artikel: „Wie der Chef des Bundesnachrichtendienstes seine Behörde umkrembelt.“ – „Ein Mensch, der bis in die Fingerspitzen professionell agiert und der sich genau überlegt, wann er sich Gefühle erlaubt.“ – „Von Hannings Rückgrat erzählen seine Kollegen.“

Und dann muss ich noch einmal den Vorspann des Artikels in der [Süddeutschen](#) vom 17.12.2006 lesen, der den „Bundestrojaner-Hoax“ in die Welt gesetzt hat: „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau.“ Die Autorin diesen Unfugs ist [Annette Ramelsberger](#) – genau die, die auch die Halleluja-Orgie über Hanning geschrieben hat.

Jetzt darf man drei Mal raten, wer der Informant Ramelsbergers dafür war, dass das BKA angeblich schon unsere Rechner durchsuchen kann...

Nachtrag 30.12. Dazu [passt](#): „Redakteure würden sich gebauchpinselt fühlen, wenn ihnen Vertreter der Sicherheitsbehörden hin und wieder Informationsbröckchen zuwerfen, und sich diese „Quellen“ nicht verbauen wollen.“

24C3 | Gezielte Trojaner-Attacken



Laut [Heise](#) hat [Maarten Van Horenbeeck](#) eine schöne Geschichte über Chinesen-Trojaner erzählt. Ich glaube das alles nicht so einfach. Natürlich: Wenn man „The Month of Kernel Bugs „([MoKB](#)) archive“ anschaut, überkommt einen das Gruseln. Dennoch: Ich halte die meisten Meldungen, die Chinesen hätten wieder irgendetwas „gehackt“, für reine Propaganda, weil niemand die Faken überprüft. (vgl. [spiggel.de](#), 04.09.2007: „Chinesen greifen das Pentagon an!“ sowie [spiggel.de](#), 26.08.2007: „Die China-Hacker kommen nicht“).

„Laut Van Horenbeeck startete die immer wieder mit China in Verbindung gebrachte Trojaner-Invasion 2005 mit einem unauffällig per E-Mail dahergekommenen Bildschirmschoner-Objekt mit dem Namen [dot.scr](#), das eine ausführbare Datei erhielt.“ So ein Quatsch: Warum soll ein Attachment

„unauffällig“ sein? Und wer installiert Bildschirmschoner von unbekanntem Absendern, womöglich aus China? „2006 folgte gemäß



Van Horenbeeck ein nach wie vor aktiver Trojanerangriff mit einer als [HuJintao.doc](#) betitelten Word-Datei.“

Ein Hacker-Angriff mit einer Word-Datei? Womöglich mit einem Bambus-Rechner? Soll ich diesen Schwachfug glauben?

Laut Horenbeck sei die Windows-Schwachstelle [MS05-035](#) ausgenutzt worden. Nach [Heise](#) befasst sich MS05-035 „... mit einem Fehler in der Font-Behandlung von Word, der sich durch manipulierte DOC-Dateien ausnutzen lässt. Betroffen ist Word aus Office 2000 und XP (2002) sowie die Word-Versionen aus Microsoft Works 2000 bis 2004. Word 2003 hingegen ist laut Microsoft immun.“ Sehr gefährlich hört sich das nicht an, denn es betrifft nur einige Systeme – und die müsste jemand vorher kennen.

„Im April erregte ein ungewöhnlicherweise in einem reinen HTML-Anhang daherkommender Trojaner die Aufmerksamkeit des Belgiers.“ Mir scheint dieser Belgier ein Wichtigtuer zu sein, mit Verlaub. Anhang in HTML! Da lachen ja die Hühner! Wie

巡视员讲话：
<http://202.113.70.7/download/zhangxuehai.doc>
雷克俭同志讲话：
<http://202.113.70.7/download/leikejian.doc>

胡锦涛《在新时期共产党员先进性专题报告会上讲话》
<http://202.113.70.7/download/hujintao.doc>
江泽民论加强和改进执政党建设《专题摘要》
<http://202.113.70.7/download/jiangzemin.doc>

理工大学实施方案
<http://202.113.70.7/download/fangan.doc>

sollte man jemanden, der mit seinem MUA vernünftig umgehen kann, damit überlisten können – und dann vielleicht auch noch *ohne* Javascript? Nein, nein, nein, ich glaube weiterhin kein Wort.

Eine wichtige Quelle für die angeblichen Trojaner-Angriffe aus China ist jemand, der keinen Anlass auslöst, um sich zu blamieren: „Die Beamten im Innenministerium haben die angeblich aus China stammenden Trojaner-Angriffe auf Bundesbehörden nachdenklich gemacht. ‚Finstere dritte Mächte‘ hätten entsprechende Versuche unternommen, weiß Staatssekretär [August Hanning](#). Diese seien aber „erfolgreich abgewehrt worden“. ([Heise](#)-Newsticker, 05.09.2007)

Vielleicht wäre es an der Zeit, wenn der geschätzte Kollege Krempl, der fast alle die Meldungen bei Heise verfasst hat, die Zeit fände, auch einmal die Fakten zu überprüfen – dann löste sich der Trojaner-Hoax made in VR China vermutlich in Luft oder in [Praktikanten](#) auf.

24C3 | Hackerfreiräume und

Anonymisierungsdienste

[Heise Newsticker](#): „24C3: Hackerfreiräume und Anonymisierungsdienste“

„(...) Ein Tor-Server-Betreiber der German Privacy Foundation ([GPF](#)) hatte [jüngst](#) davor gewarnt, dass privat unterhaltene Rechner für das Anonymisierungsnetzwerk aufgrund der strengen strafprozessualen Anforderungen aus dem heftig umstrittenen Gesetz zur Neuregelung der Telekommunikationsüberwachung kaum noch aufrecht erhalten werden könnten. Dabei sind sich Experten einig, dass über DSL betriebene, auch nur zeitweilig für Tor geöffnete Ausgangsknoten (Exit Nodes) wichtig sind für das gesamte Anonymisierungsnetz. Hintergrund ist, dass sie keine statische IP-Adresse haben und somit weniger leicht auf eine Filterliste von Zensoren wandern können.

Trotzdem gab [Mittenzwei](#) das Motto „keine Panik“ aus. Zum einen würden alle Bestimmungen aus der Gesetzesnovelle erst 2009 mit Bußgeldern durchgesetzt. „Wir können sie bis dahin komplett ignorieren.“ Bis zum Stichtag könne dann die ein oder andere Verfassungsbeschwerde gegen die Vorratsdatenspeicherung greifen. (...)“

Man kann nicht alles haben: Der *Betreiber* [unserer Torserver](#) (mittlerweile zwei, und vier von Mitgliedern) ist der Verein, Karsten ist der Admin.

Die Wut auf Google

[Futurezone.orf.at](#): „Die Wut auf Google“ – „Ihr spinnt wohl alle‘ und ‚Vertrauen der Kunden verspielt‘ schreiben erboste Benutzer in den Google-Foren. Eine neue Web-2.0-Funktion zeigt

allen Gmail-Kontakten automatisch an, welche Nachrichten der betreffende Benutzer abonniert hat.“

Wer hier spinnt, ist ja wohl klar: Diejenigen, die Gmail nutzen, ob mit oder ohne das [Feature](#). Man muss nur die [AGB](#) lesen: „Die inhaltliche Zuordnung von Anzeigen ist ein vollständig automatisierter, von Computern durchgeführter Prozess“.

Ja, und die Erde ist eine Scheibe – als wenn es *darauf* ankäme! Die Software liebt euch doch alle...

24C3 | Volldampf voraus

[CCC Events Weblog](#) über den CCC-Kongress 2007 unter dem Motto „Mit Volldampf voraus“. [[Übersicht aller Blogs](#)]

Mitglieder der [German Privacy Foundation](#) treffen sich am Freitag, 28.12., um 17.00 Uhr vor dem [Kongresszentrum](#) [vgl. Diskussion und Infos im [internen Forum](#)] .

Die Partei hat immer recht

Laut [Heise](#) hat Bundespräsident Köhler das Gesetz zur Telekommunikationsüberwachung und Vorratsdatenspeicherung unterzeichnet. „Es gab keine durchgreifenden verfassungsrechtlichen Bedenken...“ Quod erat demonstrandum.

German Privacy Foundation proudly presents:

Die [German Privacy Foundation](#) hat den zweiten [Tor-Server](#) in Betrieb genommen: **gpftor1** echo931.server4you.de [85.25.141.60] und **gpftor3**.privacyfoundation.de [91.121.102.64, in Frankreich]. Nr. 2 ist under construction...