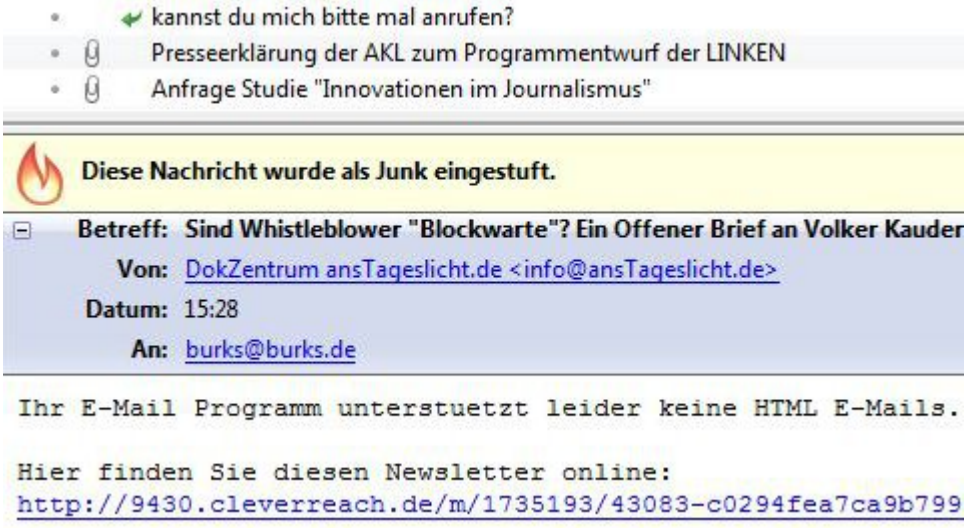
# Diese Nachricht wurde als Junk eingestuft, revisited

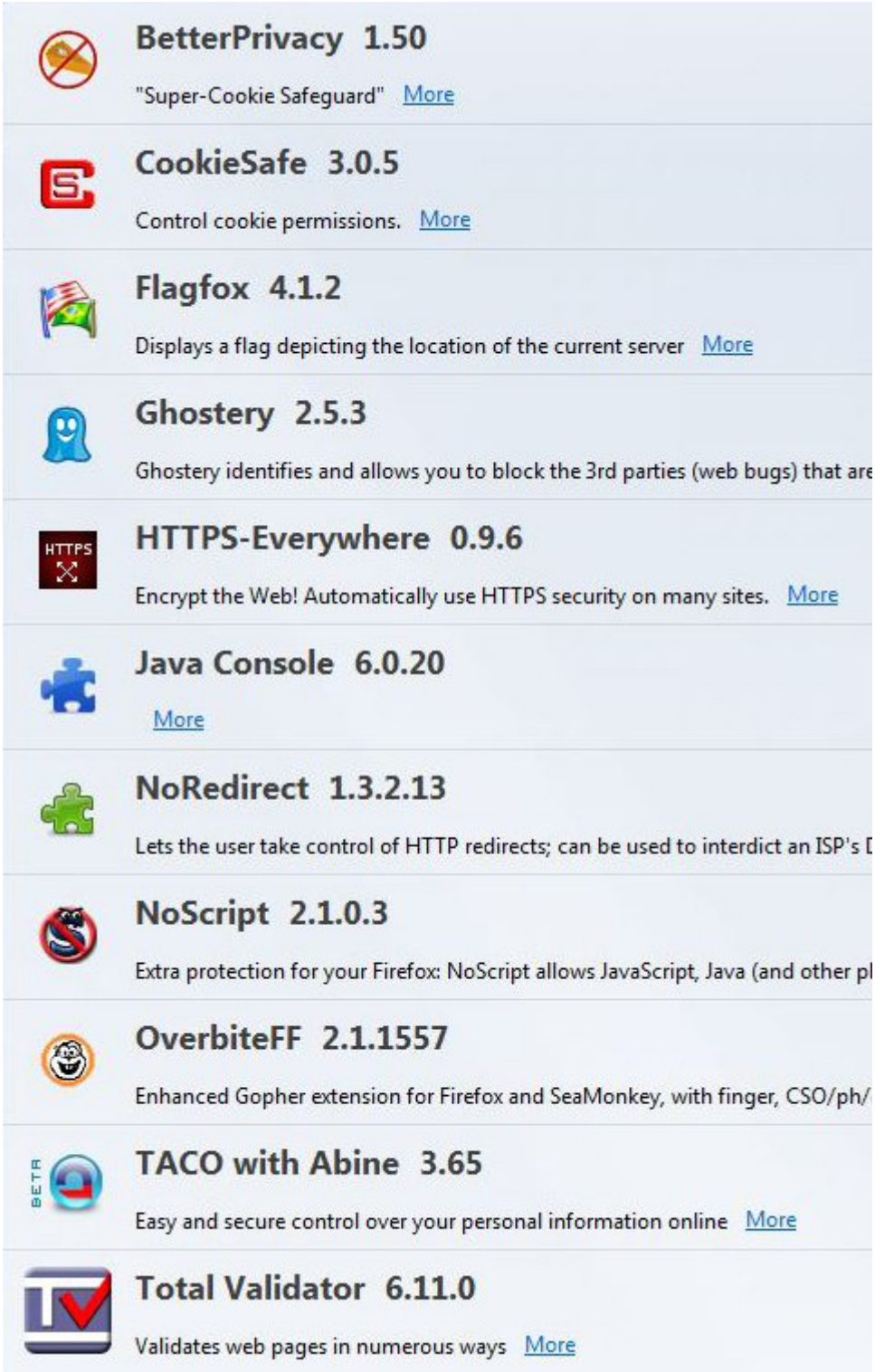



Wieso „leider“, ihr Dödel? Ich habe das ausgestellt und verboten! Ich lese E-Mails *niemals* in HTML, da könnte etwas Böses oder etwas noch Böseres enthalten sein.

Guckst du hier:
„HTML-Mails werden teils ungewollt und unbewusst durch die Voreinstellung des verwendeten E-Mail-Programms, insbesondere von Microsoft-Programmen, versandt, teils bewusst, um Schriftauszeichnungen verwenden zu können, etwa in E-Mail-Newslettern. Obwohl das HTML-Format standardisiert ist, war es ursprünglich nicht für den Einsatz in E-Mails gedacht. (…) HTML-Mails stehen im Ruf, unsicherer als reine Text-Mails zu sein. Da die Vergangenheit gezeigt hat, dass das Rendering von HTML-Mails anfälliger für Sicherheitslücken ist als die Anzeige von Klartext, empfehlen auch heute noch viele EDV-Ratgeber und Softwarehersteller die HTML-Anzeige von E-Mails zumindest im Vorschaufenster des E-Mail-Programms zu deaktivieren oder ganz auszuschließen.“

Davon habt ihr Spammer und Phisher natürlich noch nie etwas gehört. Ich bin aber keine Pappnase wie ihr es seid.

# Aktive Inhalte




Gober Unfug auf der Website der Sirrix Ag, die uns den „Browser in the Box“ andrehen will – laut Heise ein „Sicherer

Browser für Privatanwender und Unternehmen“:

„Spätestens seit das Internet mit ‚Web 2.0‘ aktiv wurde, ist die Gefahren – Nutzen Balance verloren gegangen. ‚Aktive Inhalte‘ sind aus heutigen Webseiten nicht mehr wegzudenken, moderne Webseiten sind von vollwertigen nativen Anwendungen kaum noch zu unterscheiden. Programmierschnittstellen wie JavaScript, Java, ActiveX oder VBScript erlauben auch den Zugriff auf den PC des Benutzers, etwa auf das Dateisystem oder eine angeschlossene Webcam. Trojaner und Viren können damit neue mächtige Werkzeuge zum Zugriff auf vertrauliche Daten missbrauchen.“

So ein Quatsch. Ich lasse „aktive Inhalte“ schlicht nicht zu. Wenn Webdesigner nicht in der Lage sind, korrektes HTML zu schreiben oder mir keine barrierefreie Version anbieten, dann umsurfe ihr ihr Machwerk eben weiträumig. Ich frage mich, warum das BSI sich für einen solchen Unfug hergibt. Ich bin auch nicht der Meinung, dass Behörden des Bundes mit Firmen zusammenarbeiten sollen.

Man sollte einen vernünftigen Browser benutzen und den vernünftig einstellen (aktive Inhalte verbieten, insbesondere Javascript), und das war’s dann. Man kann natürlich auch das Schloss vor die Tür nageln…

---

# Lena in Gefahr – Terror-Alarm in Deutschland [2. Update]


Es fällt mir immer schwerer, *nicht* von gleichgeschalteten Medien in Deutschland zu sprechen. Der Vergleich hinkt natürlich, weil die Vorzensur aus der Schere in den Köpfen besteht, kombiniert mit Dummheit und Faulheit. Niemand zwingt Journalisten dazu, gequirlten Unsinn zu schreiben. (Ich dürfte gar nicht meckern, hätte ich doch einen guten Artikel selbst schreiben zu können, aber ich bin gestern zu spät ins Bett gegangen.)

Ich habe mir also zum Frühstück das angeschaut, was mir als „Nachrichten“ und „Fakten“ zum Thema „Terrorgefahr in Deutschland“ angeboten wird. Dass Stefan Krempl bei Heise das Märchen von den „heimlichen Online-Durchsuchungen“ wieder aufwärmt, wundert mich jedoch nicht.

Mit „gleichgeschaltet“ meine ich: Das, was eine Behörde verlautbart, wird unkritisch übernommen (inklusive der suggestiven Sprachregelungen), ohne zu überprüfen, ob die Fakten stimmen. Im Sozialismus hieß eine derartige „Quelle“ schlicht „Agitprop“. Wenn viele Medien voneinander abschreiben, gilt eine These offenbar als verifiziert. Das war auch schon beim Thema Online-Durchsuchung so. Die Rheinische Post schießt den Vogel ab und gibt es auch noch zu: „Übereinstimmenden Medienberichten zufolge sollen die Festgenommenen einen größeren Anschlag in Deutschland geplant haben“. Dann *muss* es ja wahr sein, wenn alle anderen des Kaisers neue Kleider bewundern!

„Den Angaben zufolge wurde die Kommunikation der Männer überwacht. (…) Amid C. sei dafür verantwortlich gewesen, die ‚verschlüsselte und konspirative Kommunikation‘ untereinander

sicherzustellen. Laut Ziercke war es den Behörden jedoch mit umfangreichen, monatelangen Überwachungsmaßnahmen gelungen, den mutmaßlichen Terroristen auf die Spur zukommen.“ (Focus) „Im Zuge der Ermittlungen hatte das BKA einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf seinem Rechner installiert.“ (Spiegel) „Das Bundeskriminalamt (BKA) ist den mutmaßlichen Terroristen durch Überwachung ihrer Handys und Computer auf die Spur gekommen.“ Süddeutsche) „Bei den Ermittlungen hatte das BKA dem „Spiegel“ zufolge einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf dem Rechner des Verdächtigen installiert.“ (FTD) „Den Angaben zufolge wurde die Kommunikation der Männer überwacht.“ Mitteldeutsche Zeitung)

Die FTD redet also von einem „Bundestrojaner“. Was aber soll das sein? Man kann einen Computer nur fernsteuern und überwachen, wenn man a) einen physikalischen Zugriff auf ihn hatte, b) wenn der Besitzer des Computers denselben nicht geschützt hatte und c) haben die Ergebnisse, die durch Spionage-Software auf einem Rechner gewonnen wurden, vor Gericht keinerlei Beweiswert, weil diese den Computer verändert. Man kann das vergleichen mit einem V-Mann, der eine Neonazi-Kameradschaft gründet und diese dann auffliegen lässt. (Darüber habe ich ein ganzes Buch geschrieben.)

Die Taz gibt sich wenigstens Mühe: „Permanent waren 50 Leute in Observationstrupps und weitere 76 Beamten für sonstige Überwachungsmaßnahmen im Einsatz. Dabei wurden Wohnungen und Telefone abgehört, Emails mitgelesen. Auf Computern wurden Spähsoftware installiert und verschlüsselte Internet-Telefonate wurden schon im Computer, also vor der Verschlüsselung (mittels Quellen-TKÜ) erfasst.“

Aha. Bei der angeblichen „Online-Durchsuchung“ wird es sich um das Abhören von Skype gehandelt haben. Verschlüsselte E-Mails kann man nicht lesen, es sei denn, man hätte einen Keylogger installiert und protokollierte die Tastatur-Anschläge a priori

mit. (By the way, taz: „Quellen-TKÜ“ ist Neusprech des Wahrheitsministeriums.)

Und was lehrt uns das alles? Schauen wir doch ein wenig genauer hin, um hinter den Nebelkerzen ein paar winzige Fakten erkennen zu können.

„Dort habe er von einem ‚hochrangigen Al Qaida-Mitglied‘ den Auftrag bekommen, einen Anschlag in Deutschland auszuführen. Wer der Auftraggeber konkret war, wollten weder Ziercke noch Bundesanwalt Rainer Griesbaum sagen. “ (taz) Ich weiß, wer es war – Adil Hadi al Jazairi Bin Hamlili!

Regimetreue Medien geben der Totalüberwachungs-Lobby jetzt breiten Raum: „‚In Deutschland besteht weiterhin eine konkrete Terrorgefahr‘, sagte Uhl der ‚Welt am Sonntag‘. Gleichzeitig zeige der Fall, dass die Nachrichtendienste zu wenig Eingriffsrechte besäßen. Denn die entscheidenden Hinweise erhielten die deutschen Ermittler von der amerikanischen CIA. (…) ‚Wir müssen wissen, mit wem die Terroristen kommunizieren, um ihre Netzwerke ausfindig machen zu können‘, sagte er. ‚Dafür brauchen wir die Vorratsdatenspeicherung.'“

Passt schon. Wir haben verstanden.

Vermutlich wird bei der Gerichtsverhandlungen, die vielleicht noch in diesem Jahr stattfinden, von den Vorwürfen nicht viel übrig bleiben. Aber das wird dann im Kleingedruckten stehen, das niemand mehr liest: „Bei der Hausdurchsuchung wurde kein Sprengstoff gefunden. Außerdem stellte das BKA fest, dass der Plan zur Herstellung eines Zünders gar nicht hätte gelingen können, weil die Terrorbastler die falschen Grillanzünder gekauft hatten.“

Wie das? Stehen im Internet denn *falsche* Bombenbauanleitungen? Gehört es denn nicht verboten, *falsche* Bombenbauanleitungen zu verbreiten? (Akte aka Ulrich Meyer, übernehmen sie: „Es war unser Thema am vergangenen Donnerstag: Bombenbauanleitungen im Internet. Das Netz ist voll davon, Spezialisten haben über

eine eigene Filtersoftware 680.000 Seiten weltweit aufgestöbert“.)

„Dennoch erließ die BGH-Ermittlungsrichterin gegen alle drei Beschuldigte Haftbefehle.“ Quod erat demonstrandum.

Mich wundert, dass alle Medien, sogar die Krawallblätter, sich die einmalige Chance entgehen ließen, das Volk auf die anlass- und verdachtsunabhängige Totalüberwachung aka Vorratsdatenspeicherung mental einzustimmen. „Unterdessen verlautete aus Sicherheitskreisen, dass die drei Terrorverdächtigen einen Anschlag auf den Eurovision Song Contest geplant haben könnten. Allerdings hätten die Verdächtigen nicht konkret darüber gesprochen, hieß es.“ (Welt)

Burks.de hat daher die dazu passenden Schlagzeile gewählt.

„Sicherheitskreise“: Das sind die Geheimdienstler, die Journalisten auf ihrer Gehaltsliste haben oder wissen, dass diese geschmeichelt sind, wenn man ihnen angebliche „vertrauliche Vorab-Informationen“ zukommen lässt und die daher gern bereit sind, Agitprop, die man gern verbreitet hätte, Wort für Wort ohne Kritik zu publizieren.

„Die Terroristen wollen Lena umbringen. Das haben sie zwar nicht so gesagt, aber es könnte ja sein. Würden Sie das bitte so bei Welt Online veröffentlichen? Danke.“

*Update*: EFF: „New FBI Documents Provide Details on Government’s Surveillance Spyware“. „The documents discuss technology that, when installed on a target’s computer, allows the FBI to collect the following information“..blabla..und wie bekommt man das auf den Computer des Zielobjekts?

Guckst du hier (burks.de, 31. Juli 2007):

„… es geht um CIPAV: „FBI-CIPAV.exe Is an Unknown Application. Install Anyway?“ Jetzt aber im Ernst: „Die Abkürzung steht für

„Computer and Internet Protocol Address Verifier“, zu Deutsch: Computer- und Internet-Protokoll-Adressen-Verifizierer. Dieses Programm ist in der Lage, auf dem Rechner des Verdächtigen die Internet-Verbindungen und angesteuerten Homepage-Adressen samt Datum und Uhrzeit aufzuzeichnen. Die in Fachkreisen Trojaner genannte Software erfasst auch weitere Daten wie das Betriebssystem des ausgehorchten Computers, den Namen des bei der Windows-Registrierung angegebenen Nutzers, Teile der Windows-Registrierungsdatenbank oder eine Aufzählung aller laufenden Programme. Im vorliegenden Fall übermittelte CIPAV einige dieser Informationen per Internet an die FBI-Rechner.“ Das ist aber ein ultraböhzes Programm, fast so böse wie das Betriebssystsem, auf dem es nur läuft.

Wired dazu: „[1] the FBI sent its program specifically to Glazebrook’s then-anonymous MySpace profile … [2] „The CIPAV will be deployed through an electronic messaging program from an account controlled by the FBI. The computers sending and receiving the CIPAV data will be machines controlled by the FBI.“ … [3] More likely the FBI used a *software vulnerability*, either a published one that Glazebrook hadn’t patched against, or one that only the FBI knows.“ Genau, Software-Lücken, von denen nur das FBI etwa weiß. (…)

Die *Welt* betont sehr deutlich, dass der Schüler offenbar „arglos“ etwas abrief, vermutlich so, wie das *Welt*-Redakteure machen mit ihrem Outlook und dem unverschlüsselten und mit Javascript-gespickten Spam, den sie das immer bekommen. Der Artikel ist also ein Schmarrn. Ich darf auf mein Blog vom 19.07.2007 hinweisen („Heise Hoax-verseucht“), in dem die Details zu CIPAV abgehandelt werden.“

*2. Update*: New York times: „Bild, Germany’s most widely read and generally reliable (sic!) newspaper, reported that the terrorist cell might have planned to hit the popular Eurovision Song Contest on May 14, though that event’s organizers said they had not been alerted to any such threat. „>. Qood erat demonstrandum. (via Überschaubare Relevanz)

# Fehler: Umleitungsfehler oder: Die nie beendete Anfrage

Nur damit das klar ist: Ich bin *nicht* schuld. Wenn etwas nicht funktioniert, muss ich mir *nicht* einen Browser herunterladen, ich muss *nicht* die Sicherheitseinstellungen verändern. Nein. Nie.

Die Betreiber der Website, die ich *nicht* ansehen kann, sind schuld. Es sind Trottel, DAUs, Ignoranten oder sie wollen mich, ohne dass sie mir das verraten, ausspionieren. Es ist *nicht* selbstverständlich, dass jemand Cookies per default gestattet, es ist *nicht* selbstverständlich, dass jemand Javascript per default erlaubt. Merkt euch das!

Ich muss *nicht* den Traffic auf euer bescheidenen Website erhöhen; ich kann auch woanders hingehen. Es ist wie im realen Leben: *Ich* bleibe so, wie ich bin, und wenn euch das nicht gefällt, dann müsst *ihr* euch ändern oder den Kontakt mit mir vermeiden. (So, jetzt geht es mir wieder besser und genug Kaffee habe ich jetzt auch getrunken.)

Ich darf auch an mein Posting vom November 2008 erinnern: „Ein einfaches Sicherheitskonzept für Daten“ sowie an das vom Dezember 2010: „Browser-”Lücken” – Experte ist nicht alarmiert“.

# Bgsound

Golem: „Stefan Münz, der mit Selfhtml über viele Jahre für die deutschsprachige HTML-Referenz verantwortlich war, hat ein Handbuch zu HTML5 veröffentlicht. Das Ende 2010 erschienene Buch steht nun auch online kostenlos zur Verfügung."

Ich habe mal ein bisschen gestöbert und bin auf das hübsche Kapitel „proprietäre Elemente" gestoßen. Hihihi. Wer benutzt heute eigentlich noch *blink*?

Bei *bgsound* musste ich grübeln: „Wird heute, wenn überhaupt noch gewagt, meistens mit Hilfe von Flash realisiert, das über JavaScript mit dem Event-Handler onload gestartet wird."

Mal abgesehen davon dass es dreist ist, den ahnungslosen Surfer mit Musik zwangsweise zu bedudeln: Ich surfe bekanntlich nicht wie ein DAU, sondern *ohne* Javascript. Wie erzwinge ich denn Hintergrundmusik ohne Flash und Konsorten?

---

# Like-jacking, Click-Jacking, Link-Diebstahl


Das folgende Video enttarnt diesen Trick mit Hilfe der Firefox-Erweiterung Web Developer:

**Fehler Video-/Audio-Datei**
Zur Wiedergabe benötigen Sie eine aktuellere Version des Adobe Flash Player
den Sie kostenlos für alle gängigen Betriebssysteme herunterladen können.

S 614 / C 1667
Der Rest ist dann nur noch eine Frage des richtigen Social Engineerings. Ein reißerischer Titel wie "Beim Web-Cam-Strip erwischt" weckt ausreichend Neugier,

Heise Security beschäftigt sich heute mit „Like-Jacking", das

eher als Clickjacking – zu deutsch: „Link-Diebstahl“ – bekannt ist. Ein Dau klickt auf irgendetwas, und es geschieht etwas, was er/sie nicht vermutet hat – und dann passiert etwas Böses.

Die Wired schreibt ganz richtig dazu: „Every time darkside hackers make up a new exploit, somebody’s got to make up and promulgate a new name to the security community. ‚Like-jacking.‘ You ‚like‘ something on Facebook, you get hijacked.“

Mit Leuten, die Facebook nutzen, sollte man kein Mitleid haben. Da das Datensammeln und deren -verkauf das Geschäftsmodell der sogenannten „sozialen Netzwerke“ ist, darf man sich nicht wundern. Nur wenn andere das auch tun, regt man sich offenbar auf.

Was mich immer ärgert, dass in Artikeln, die darüber berichten, so getan wird, der Nutzer sei immer und grundsätzlich total bescheuert. Nein, ist er nicht. Ich bin doch nicht so blöd und surfe mit eingeschaltetem Javascript?! Nein, ich benutze bei allen Betriebssystemen die Firefox-Erweiterung noscript und gestatte nur ganz wenigen Websites, Scripte auszuführen. Damit bin ich auf der sicheren Seite.

Warum bekommt ich also bei „Heise Security“ die Falschmeldung „Fehler Video-/Audio-Datei – Zur Wiedergabe benötigen Sie eine aktuellere Version des Adobe Flash Players, den Sie kostenlos für alle gängigen Betriebssysteme herunterladen können“? Weil sich sogar die Webdesigner dort überhaupt nicht vorstellen können, dass jemand mit einem abgeschotteten Browser surft und über die zahllosen Warnungen, was alles Böses geschehen könnte, nur schmunzelt. Klickibunti ist eben Standard, und die Nutzer werden weiter so erzogen, das als eine Art Naturkonstante anzusehen.

# Was Vorratsdaten über uns verraten

Zeit.de: „Interpol und Deutsche Bank, FBI und Scotland Yard, Flensburg und das BKA, haben unsere Daten da“, sangen Kraftwerk 1981 in Computerwelt. Es klang damals unglaublich, später bedrohlich, und heute klingt es lächerlich. (…)

Der Grünenpolitiker Malte Spitz hat sich daher entschlossen, seine Vorratsdaten aus dem Zeitraum August 2009 bis Februar 2010 zu veröffentlichen. Um sie zu überhaupt bekommen, musste er gegen die Telekom klagen. Die Daten, die *Zeit Online* hier zum Download zur Verfügung stellt und die Basis der hier gezeigten interaktiven Karte sind, entstammen einem Exceldokument mit 35.831 Zeilen. Mehr als 35.000 Mal also hat sein Mobiltelefon in diesem halben Jahr Informationen Preis gegeben… (…)

Vorratsdaten zeigen, wer Freund ist und wer Familie, sie bringen geheime Liebschaften ebenso ans Licht wie verborgene Netzwerke.“

(Vorsicht! Um die interaktive Karte ansehen zu können, muss man Javascript erlauben: Man muss sich von googleapis.com, von gstatic.com und google.com ausspionieren lassen. Das verrät uns *Zeit online* aber nicht, es wird als selbstverständlich vorausgesetzt.)

---

# Ebay-Eliza


„Vielen Dank für Ihre Nachricht. Sie haben uns mitgeteilt, dass Sie keinen Artikel einstellen können. Sie benutzen den Browser Firefox 3.6.6. Gern helfe ich Ihnen.
Die Ursache scheint ein Add-On zu sein, das Sie für Ihren Browsers Firefox verwenden, um Anzeigen zu blockieren. Ich empfehle Ihnen, die eBay-Seiten bis auf Weiteres mit dem Internet Explorer aufzurufen.
Außerdem sollten Sie ActiveX-Elemente, Java und JavaScript dulden, damit das Verkaufsformular problemlos funktioniert.“

Vermutlich war das eine Art ebay-Eliza. Wer mir rät, den Internet Explorer zu benutzten und alle Sicherheitsfeatures auszuschalten, gehört doch unter ärztliche Aufsicht. Ich werde meinen Account bei ebay jetzt kündigen.

---

# Ab heute wird geflattrt

Ich habe mich entschieden, bei Flattr teilzunehmen. Wer noch nicht weiß, was das ist, kann bei Wikipedia lesen: „Flattr ist ein Social-Payment-Service mit Sitz in Malmö, Schweden, bei dem der Benutzer monatlich einen frei wählbaren Abonnementsbetrag auf ein Konto einbezahlt. Die Medienanbieter platzieren auf ihrer Website einen Flattr-Button, den der Nutzer anklicken kann, wenn ihm der Internet-Inhalt gefällt. Am Monatsende wird der Abonnementsbetrag des Nutzers gemäß

seinen Klicks an die Medienanbieter verteilt.“

Ich bin gespannt, ob meine Artikel irgendjemandem etwas wert sind. Die beiden besten Artikel, die ich jemals geschrieben habe, habe ich im nachhinein auch geflattrt:

– Projekt Xanadu, reloaded
– Die Erlkönigin

Der Button funktioniert ohne Javascript. Es gibt auch einen allgemeinen Spendenknopf auf der rechten Spalte.

---

# Internet-Quiz

Wie steht es um Ihre Internet-Grundkenntnisse? Sie kennen sich mit dem Internet schon aus? Aha. Dann beantworten Sie schnell die folgenden Quiz-Fragen:

☐ja
☐nein Ich kenne den Unterschied zwischen dem Internet und dem World Wide Web.

☐ja
☐nein Ich kenne die Boolesche Algebra einer Suchmaschine.

☐ja
☐nein Ich benutze PGP bzw GnuPG. weil ich nicht nur elektronische Postkarten verschicken will und weil ich keine Webcam im Schlafzimmer habe

☐ja
☐nein Ich benutze einen Newsreader, um abonnierte Newsgroups zu lesen.

☐ja
☐nein Ich weiß, wie man im Usenet ein Userprofil erstellt.

□ja
□nein Ich weiß, welche Software man für IRC benutzt und kann verschlüsselt und unbeobachtet chatten.

□ja
□nein Ich weiß, warum man einen TOR-Schlüssel nicht beim Hausmeister abgeben muss.

□ja
□nein Ich kann die IP-Adresse eines SMTP- oder News-Servers einer Firma zuordnen.

□ja
□nein Ich weiß, wie man Javascript ausschaltet und wofür das gut ist.

□ja
□nein Ich weiß, was ein „Thread“ ist.

□ja
□nein Ich benutze nicht Webmail, sondern einen vernünftigen MUA. SCNR

□ja
□nein Ich kann einem DAU erklären, warum man für „Phishing“ keinen Angelschein braucht.

Antworten:
„Ja“ 12 mal: Sie sind Mitglied in der „German Privacy Foundation“ und inkognito hier.
„Ja“ 9-11 mal: Sie sollten vielleicht eher einen technischen Beruf ergreifen – der wird besser bezahlt. Bewerben Sie sich als Sysop (was ist das?) beim Innenministerium!
„Ja“ 6-8 mal: Sie sind nicht unbedarft, aber können noch etwas dazulernen.
„Ja“ 3-5 mal: Rudimentäre Vorkenntnisse sind vorhanden, aber ausbaufähig.
„Ja“ 0-3 mal: Sie haben keinen blassen Schimmer vom Internet, behaupten aber vermutlich das Gegenteil. Sie sind wahrscheinlich ein Journalist mit Facebook-Account, der über „Online-Durchsuchungen“ Artikel schreibt.

[vgl. Heise: „Studie: Wachsende Sorge um ‚digitale Außenseiter' – …sind 63 Prozent der Gesellschaft nicht oder wenig souverän im Umgang mit der digitalen Technik". Ich halte den Wert von 90 Prozent für wahrscheinlicher.]

---

# Firesheep oder „Hacken" für jedermann

Zuerst habe ich mich bei der Lektüre des aktuellen Print-Spiegels geärgert, dass jemand unwidersprochen dummes Zeug über das Internet verbreiten durfte. Der „Strafrechtler und Schufa-Ombudsmann Winfried Hassemer: „Wer zwei Stunden im Internet surft, hinterlässt mehr Spuren als bei der Schufa." Nein. Stimmt nicht. Gar nicht wahr. Nur DAUs hinterlassen Spuren und erlauben Cookies und Javascript und HTTP referrer. Aber so ist nun mal leider das Niveau der Diskussion. Es ist zum Heulen.

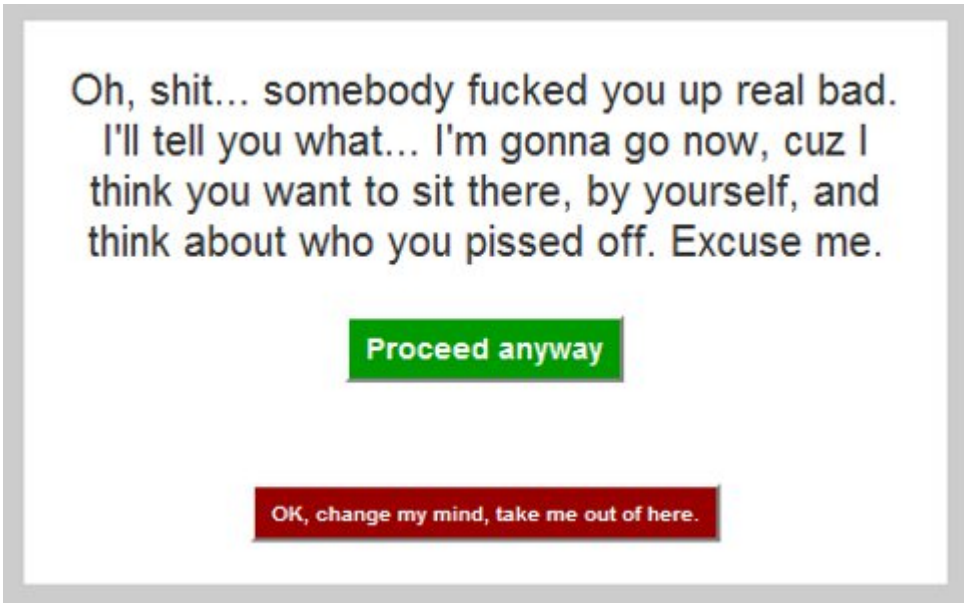
Unter der reißerischen Überschrift „Hacken für jedermann" lesen wir auf S. 131 etwas über Firesheep, „a Firefox extension that demonstrates HTTP session hijacking attacks". Kein Wort darüber in Spiegel Offline, was diese Software macht, sondern nur dumpfe Panikmache: „Automatisch schnüffelt sie nach ungesicherten Verbindungen in der Umgebung, zum Beispiel um auszuspähen, der sich im Café über ein ungeschütztes WLAN bei Facebook angemeldet." Vermutlich kann man mit diesem „Hacker-Tool" auch Verkehrsampeln ausstellen….

Warum sollte man jemanden warnen oder mahnen, der bei Facebook ohnehin die Hosen runterlässt und seine Daten in alle Welt verstreut (was war noch mal das Geschäftsmodell von Facebook?)…. Bruce Schneier hat dazu das Nötige gesagt:

„Basically, Facebook authenticates clients with cookies. If someone is using a public WiFi connection, the cookies are sniffable. Firesheep uses wincap to capture and display the authentication information for accounts it sees, allowing you to hijack the connection.(…) Protect yourself by forcing the authentication to happen over TLS. *Or stop logging in to Facebook from public networks*.“

---

# No script!





Dieser Beitrag ist den unbelehrbaren DAUs gewidmet, die

meinen, man müsste Javascript beim Surfen einschalten. Und den Webdesignern, die zum Thema Sicherheit ein Verhältnis haben wie Klaus Störtebeker zum Handelsrecht. Wer auf die Screenshots klickt, lernt etwas.

---

# All your data belong to us


Heise: „Das Bundesministerium des Innern (BMI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben eine Studie zum Identitätsdiebstahl und -missbrauch im Internet veröffentlicht. Das mehr als 400 Seiten starke Dokument betrachtet Identitätsdiebstahl und Identitätsmissbrauch aus technischer und rechtlicher Perspektive und leitet daraus Handlungsempfehlungen ab."

Ich habe es mir mal angesehen, auch unter dem Aspekt der real gar nicht existierenden „Online-Durchsuchung".

„Prinzipiell kann eine Infektion durch jegliche installierte Software auf dem Client-System stattfinden, die beispielsweise veraltet und daher auf irgendeiner Art und Weise verwundbar

ist. Bei ihren Untersuchungen fand die Firma Trusteer des Weiteren heraus, dass auf fast 84 Prozent der Rechner eine verwundbare Version des Adobe-Readers installiert war. Durch bösartige pdf-Dokumente ist es so möglich, auf dem Endsystem des Nutzers Schadcode auszuführen. Natürlich. Hängt aber vom Betriebssystem und vom Browser ab. Frage: woher bekommt der Angreifer die (jeweils persönliche dynamische!) IP-Adresse des Zielobjekts, das ausgespäht werden soll? „Allerdings sind bisher keine Möglichkeiten bekannt, Addons automatisiert ohne Mitwissen des Nutzers zu installieren." Aha.

„Zu einer sehr gefährlichen Infektionsmethode gehört der Drive-By-Download, die eine Schwachstelle im Browser des Opfers ausnutzt. Aber auch der Versand per E-Mail war vor einiger Zeit sehr populär. Eine weitere Methode ist, an beliebte Software ein Trojanisches Pferd anzuhängen und anschließend auf Webseiten oder über P2P-Netzwerke illegal zum Download anzubieten." Funktioniert nur, wenn das Zielobjekt selbst aktiv mitspielt und sich wie ein DBU (denkbar bescheuertste User) verhält. Frage: woher bekommt der Angreifer die (jeweils persönliche dynamische!) IP-Adresse des Zielobjekts, das ausgespäht werden soll?

„Selbst durch die Nutzung erweiterter Mechanismen wie etwa speziellen Browser-Add-Ons (beispielsweise NoScript) lässt sich kein vollständiger Schutz realisieren. Stattdessen leidet aber die Benutzerfreundlichkeit unter diesen Mechanismen, teilweise sind moderne *[was heisst hier „modern"? Das ist schlicht nicht barrierefrei! BS]* Webseiten (die zwingend *[Schwachfug BS]*auf Erweiterungen wie Javascript angewiesen sind) gar nicht mehr benutzbar. Zudem liegt das große Problem aktueller Antivirenprogramme in ihrer Reaktivität, denn sie können in den allermeisten Fällen nur Malware zuverlässig finden, die bereits bekannt ist. Technische Maßnahmen lösen zudem nicht alle Sicherheitsprobleme, vielmehr ist eine umfassende Aufklärung der Anwender von großer Bedeutung". Deswegen plädiere ich ja schon seit langem vor, die

Prügelstrafe für Webdesigner einzuführen, die einen zu Javascript zwingen wollen. Das eigentliche Problem hat also zwei Ohren und sitzt vor dem Monitor. Ich surfe grundsätzlich *ohne* Javascript. Und eine Website, die mich dazu zwingen will, boykottiere ich und stelle den Webdesigner unter den Generalverdacht, eine ignorante dämliche Pfeife zu sein.

„Cross-Site-Scripting (XSS) bezeichnet das Ausnutzen einer Sicherheitslücke in Webanwendungen, wobei Informationen aus einem nicht vertrauenswürdigen Kontext in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig gelten. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden. Ziel ist meist, an sensible Daten des Opfers zu gelangen, um beispielsweise Identitätsdiebstahl zu betreiben. Eine sehr verbreitete Methode hierfür ist, *bösartiges JavaScript* als Payload der XSS-Schwachstelle zu übergeben. Dieses JavaScript wird dann im vertrauenswürdigen Kontext im Browser des Opfers ausgeführt.“ Wie oft muss man also auf einen Webdesigner wohin einprügeln, damit er seine Finger von Javascript lässt? Javascript an sich kann nützlich sein. Wenn man aber Nutzer dazu erzieht, das nicht als Option, sondern per default aktiviert zu lassen, dann handelt man verantwortungslos.

„Die Infektion eines Clients vollzieht sich dabei in mehreren Schritten: Zunächst muss der Client bzw. dessen Anwender auf eine Website gelockt werden, auf der der entsprechende Schadcode vorhanden ist. Gerne werden dazu Websites verwendet, denen der Benutzer ein gewisses Grundvertrauen entgegenbringt.“ Frage: woher bekommt der Angreifer die (jeweils persönliche dynamische!) IP-Adresse des Zielobjekts, das ausgespäht werden soll? „Surft ein Nutzer nun auf eine solche präparierte Webseite und ist sein Browser anfällig für den dort abgelegten Exploit, so erfolgt die Übernahme des PCs.“ Vermutlich hat so man Ziercke so instruiert, und das hat das natürlich nicht verstanden und machte dann daraus: „Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem

man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht.“ – „Initialer Schritt ist, dass der Client auf die manipulierte Website herein fällt.“ Nein, nicht der Client, sondern der Homo sapiens, der ihn benutzt, den der Angreifer als Homo sapiens aber gar nicht erkennen kann, sondern nur dessen IP-Adresse.

Eine hübsche Anmerkung der Studie zum normalen Sicherheitsstandard: „Somit kann fast jedes Telefonat heute durch einen Angriff auf das Internet mitgehört werden, und Notrufnummern können durch Intenet-basierte Denial-of-Service-Angriffe lahmgelegt werden.(…) Durch das Auftreten eines neuen, besonders aggressiven Internet-Wurms (Conficker *[gilt wieder nur für Windows!]*) wurden ganze Truppenteile der Bundeswehr und der französischen Luftwaffe lahmgelegt.“

Auch schön: „Die Suche nach Passwörtern unter Google lässt sich bspw. mit dem Suchstring *intext:“password|pass|passwd“ (ext:sql | ext:dump | ext:dmp) intext:values* realisieren.“ Bruhahaha.

„Zielgerichtete Angriffe auf Linux-Client-Systeme sind nach wie vor kaum zu verzeichnen. (…) Beispielsweise sind Drive-By Angriffe auf Browser unter Linux bisher nicht bekannt.“ Nur gut, dass „Gefährder“ und andere Bösewichter so gut wie nie Linux benutzen, Herr Chef des Bundeskriminalamtes – so hat man Sie und Frau Ramelsberger doch sicher gebrieft?

Der wichtigste Satz der Studie: „Grundsätzlich kann Social Engineering als das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher oder gespielter Kontakte definiert werden. Das grundlegende Problem beim Social Engineering ist die Tatsache, dass Menschen manipulierbar und generell das schwächste Glied in einer Kette sind“.

Die Studie beschäftigt sich auch mit dem neuen Personalausweis: „Der flächendeckende Einsatz des neuen

Personalausweises allein wird Identitätsmissbrauch nicht verhindern können: Die von kriminellen Hackern eingesetzten Tools (die überwiegend auf Malware basieren, die im PC des Opfers ausgeführt wird) lassen sich sehr einfach an die bislang spezifizierten Sicherheitsmechanismen anpassen. (…) Es fehlt schlichtweg ein sicherer Betriebsmodus, in dem der Browser und der Bürgerclient ausgeführt werden können“. Das wird natürlich unsere Junta nicht daran hindern, den doch einzuführen.

„Es besteht offensichtlich ein erheblicher Bedarf an Information und Aufklärung. Es ist davon auszugehen, dass Nutzer oft über nur sehr geringes Wissen in Bezug auf die Gefahren des Internet und die Möglichkeiten zur Abwehr von Schäden verfügen.“ Ja, quod erat demonstrandum. Es ist auch davon auszugehen, dass die Nutzer nicht wissen, dass sie gar nichts wissen. Das war auch schon immer so.

Lesebefehl!

---

# Links, links, links, zwei, drei, vier


Laut WDR gibt es keine Mehrheit in NRW für Rot-Grün. Das ist auch gut so. „Demnach kommt die CDU auf 34,7 Prozent. Die SPD liegt bei 34,4 Prozent. Die Grünen sind mit 12,2 Prozent drittstärkste Kraft. Die FDP erhält 6,8 Prozent. Die Linke zieht mit 5,6 Prozent neu in den Landtag ein.“

Jetzt geht das Gehampel wieder los. Die Linke wird hoffentlich keine Minderheitsregierung tolerieren. (Sie wäre schön blöd, wenn sie das täte, aber das ist natürlich nicht ausgeschlossen – Wagenknecht ist ja dabei.) Was dann? Wenn die Grünen mit der CDU zusammenginge, gibt es für die Linke und die Piraten beim nächsten Mal noch mehr Stimmen. Und das wäre auch gut so. Große Koalition? Noch besser. Ich wette schon jetzt, dass die SPD in nullkommanix alle „Prinzipien“ über Bord wirft – was kümmert uns unser Geschwätz von gestern? Es geht nur um die Macht.

War mir gefallen würde: Ein Gesetz, das Parteien verbietet, vor der Wahl Koalitionen mit anderen auszuschließen. Wenn deutsche PolitikerInnen nicht mehr herumtönen dürften, mit wem sie alles *nicht* koalieren wollen, werden oder würden, könnten sie sich vielleicht mit den wichtigen Dingen beschäftigen.

Aber im Ernst: Claudia Roth und Sahra Wagenknecht in einem Boot? Da helfen nur noch der Weiße Hai oder gleich *das* Boot.

Es ist aber immer noch nicht klar, wer die Mehrheit hat.

# Avanti Facebook Dilettanti


Was ist das Gute an Facebook? Dass sich die deutschen Zensoren darüber aufregen und meinen, am deutschen Wesen müsse die Welt genesen: „Es kam zu einem offenen Brief an Facebook mit der Aufforderung, die Profile der Neonazis zu löschen, oder es komme zu einer Anzeige wegen Volksverhetzung. Am 17. April 2009 stoppte die Deutsche Telekom ihre Werbung auf Facebook mit Hinweis auf ‚rechtsextreme' Webseiten auf dem Portal". Was ist eigentlich daraus geworden? Deutsche Staatsanwälte verklagen Facebook wegen „Volksverhetzung" – trotz des First Amendment? Zuzutrauen wäre es ihnen. Nur mal zum Erinnern: „Der 1791 verabschiedete Artikel verbietet dem Kongress, Gesetze zu verabschieden, die die Meinungsfreiheit, Religionsfreiheit, Pressefreiheit, Versammlungsfreiheit oder das Petitionsrecht einschränken."

So etwas gibt es in Deutschland **nicht**. Der Bundestag **darf** Gesetze erlassen, die die Meinungsfreiheit, die Pressefreiheit und die Versammlungsfreiheit einschränken. Einige Grünen haben jüngst wieder schärfere Zensur-Gesetze gefordert, die Partei „Die Linke" will das Internet zensieren und das Bundesverfassungsgericht muss immer wieder eingreifen, wenn deutsche Gerichte die Versammlungsfreiheit mit Füßen treten. Aber es ist verschwendete Zeit, den Deutschen erklären zu wollen, was Meinungsfreiheit (auch für die Blösen, die Doofen

und die Ekligen) bedeutet. Das ist intellektuell zu anspruchsvoll für Lichterkettenträger.

Ich schweife ab. Zum Thema. In der aktuellen c't las ich einen interessanten Artikel über soziale Netzwerke. „Facebook hat nach eigenen Angaben mehr als 400 Millionen aktive Benutzer, von denen sich jeder zweite täglich einloggt: Wäre der Dienst ein Staat, so wäre er noch vor den USA der drittbevölkerungsreichste der Welt."

Bei Wikipedia las ich: „Ebenso überarbeitete Facebook im Dezember 2009 die Kontrolle über die Privatsphäre. Nun kann jeder Nutzer bei der Veröffentlichung von Statusmeldungen, Medien oder Links differenziert festlegen, wer diese sehen darf und wer nicht."

Ich wollte also einfach mal reinschauen, nur so aus Neugier. Die wohwollenden Leserinnen und geneigten Lesen ahnen schon, was jetzt kommt: Es ist mir nicht gelungen, trotz meines guten Willens, sogar die Standardeinstellungen meines Browsers zu verändern. Für Linux gibt es ohnehin keine „Hilfe", die diesen Namen verdient, und mein Problem, das ich gern detailliert wüsste, *was* ich an Javacsript, Cookies usw. zulassen muss, damit ich mich registrieren kann, wird nirgendwo beantwortet.

Ich bin *kein* Exot – ich bin *normal*. Ich surfe mit Mozilla/Firefox für Linux und habe die Add-Ois Cookiesafe, NoScript und RefControl in Gebrauch. Sogar wenn ich Javascript und Cookies für Facebook temporär erlaube, kann ich mich nicht registrieren – ich müsste noch zahlreiche andere aktiven Inhalte von Anbietern, die nicht kenne, auf einen Rechner lassen. Warum und wer das ist, wird mir nicht verraten. Und deshalb könnt ihr mich mal kreuzweise, ihr sozialen Netzwerke.

Update: Jetzt habe ich mein Windows-Laptop hervorgekramt…

# Summa Summarum: Politische Landschaftspflege in gelb

Spiegel Offline schreibt gewohnt linkfrei: „Westerwelles enge Verbindungen zu Unternehmern prägt auch die Auslandsreisen des Vizekanzlers. Zu Delegationen des Außenministers gehörten Manager, die zuvor an die FDP gespendet hatten. So ist bei seiner für diese Woche geplanten Südamerika-Reise Ralph Dommermuth dabei. 2005 überwies der Gründer von United Internet [*u.a. 1&1, sedo, web.de, gmx, B.S.*] 48.000 Euro an die FDP.

Bei Westerwelles Antrittsbesuchen in Estland, Japan und China im Januar war Cornelius Boersch Teil der Delegation. Der deutsche Unternehmer ist Gründer der Schweizer Beratungs- und Beteiligungsfirma Mountain Partners Group. Er hat der FDP bislang über 160.000 Euro gespendet. Bis kurz nach der Wahl war Westerwelle im Beirat eines Tochterunternehmens und kassierte dafür jährlich mindestens 7000 Euro. Zu den Gästen gehörte außerdem Miele-Chef Reinhard Zinkann. Miele ist Co-Sponsor des von Mronz vermarkteten Aachener Reitturniers."

Daraus kann man Online-Journalismus machen, Spiegel offline! Wir helfen gern und reichen die notwendigen Links nach (vgl. oben). Welches Tochterunternehmen? Dürfen wir das nicht wissen? Also müssen wir schnell recherchieren (ich schaue auf die Uhr; 16.16 Uhr). Zuerst Google: westerwelle beirat -spiegel (um die aktuelle Berichterstattung auszuschließen. Treffer 1: Guido Westerwelle (Beirat DVAG).

Das wird zu kompliziert, also bei Westerwelle nachschlagen: „Entgeltliche Tätigkeiten neben dem Mandat". Welche Tochterunternehmen hat die Mountain Partners Group, die bei

Westerwelle auftauchen? „Derzeit setzt sich der Investorenkreis aus privaten und institutionellen Investoren von den Vereinigten Staaten über Europa bis in den arabischen Raum zusammen.“ Heuschrecken. Und recht vage formuliert. Da passte Guido ja hin. Diese Frau müsste es wissen, aber heute ist Sonntag und mit E-Mails kommen die Heuschrecken nicht so richtig klar. „Diese E-Mail-Adresse ist gegen Spambots geschützt! JavaScript muss aktiviert werden“…blablabla. Internetausdruckende Heuschrecken eben.

Hm. Ich tippe auf Tellsell Consulting: „Dr. Guido Westerwelle-Beirat bei TellSell Consulting bis zum 1. Oktober 2009“. („Bis kurz nach der Wahl war Westerwelle im Beirat eines Tochterunternehmens.“) Ist das ein Tochterunternehmen der Mountain Partners Group? Bingo.

16.33 Uhr – das hat fast eine Viertelstunde gedauert. So viel Recherche kann man einem fest angestellten deutschen „Online“-Journalisten natürlich nicht zumuten. Auch der stern berichtet, widerholt aber nur, was die anderen Medien und Wikinews publiziert haben (wer von wem hier abgeschrieben hat, ist egel – es gibt keine erkennbar schöpferische Eigenhöhe bei der Recherche) und verzichtet auch darauf, den Leser per Links aufzuklären.

Westerwelle hat übrigens auf seiner Westerwelle immer noch seine Funktion als Beitrat der Tellsell Consulting stehen, obwohl er das gar nicht mehr ist. Internet-Ausdrucker – aber ich wiederhole mich.

Korruption ist laut Wikipedia auch „der Missbrauch einer Vertrauensstellung in einer Funktion in Verwaltung, Justiz, Wirtschaft, Politik oder auch nichtwirtschaftlichen Vereinigungen oder Organisationen, zum Beispiel auch Stiftungen, um einen materiellen oder immateriellen Vorteil zu erlangen, auf den kein rechtlich begründeter Anspruch besteht. Korruption bezeichnet Bestechung und Bestechlichkeit, Vorteilsannahme und **Vorteilsgewährung**.“ Die oben genannten

Unternehmen spenden der FDP und die wiederum gewährt den Vorteil, dass die Unternehmer zusammen mit dem Außenminister in die weite Welt reisen dürfen.

---

# Fehlende Frontscheibe des Browsers

„Anonym surfen im Web? Das war einmal.“ Das ist der erste Satz in einem Artikel auf Spiegel Offline. Ziemlich weit hinten kommt dann ein ganz anderer: „Noch ist der von ihnen vorgeführte Angriff relativ plump: Er dauert mehrere Minuten und erkennt Gruppenmitgliedschaften nur, wenn man kürzlich in einer Gruppe aktiv war, Cookies und Javascript aktiviert hat.“

Genau. Wer das macht, ist ein DAU wie offenbar die Redakteure bei SpOff.

Sicher Auto fahren? Das war einmal. … Allerdings verursacht man nur einen Unfall, wenn die Bremsen nicht funktionieren, ein Rad abgefallen ist und die Frontscheibe fehlt.

---

# Heute schon Pornos geschaut?

Carsten Knobloch fragt: „Heute schon Pornos geschaut?“ – „Einfach DidYouWatchPorn besuchen und den Test machen.“

Wer NoScript für Firefox benutzt, ist natürlich sicher. Die Website liest die History des Browers aus, aber nur dann, wenn Javascript eingeschaltet ist. Dödel machen das. HistoryBlock wäre auch eine Idee.

---

# Mixriot

Mit freundlichen Empfehlungen der Piratenpartei:

„Mixriot ist ein Archiv für DJ Remixes mit Schwerpunkt auf elektronischer Musik. Fast alle der über 4.000 Mixe auf der Webseite sind über zwei Stunden lang und können kostenlos als Stream gehört werden“.

(Leider nur mit Javascript abrufbar. Musiker verhalten sich bekanntlich zu Sicherheit im Internet wie Klaus Störtebeker zum Handelsrecht.)

Man muss Techno, (minimal) House und so ein Zeug mögen. Als jemand, der noch weiß, was gute Musik und guter Rhythmus sind, empfehle ich trotzdem Christopher Lawrences Album: The Gallery Podcast at Ministry of Sound 001.

Auch wenn die Jugend oft bescheuert spießig aussieht, langweilige Frisuren hat und bescheuert langweilige Musik hört: Es sei alles vergeben, wenn es in den Hörsälen der Unis so aussieht wie bei uns damals, wenn sie die richtige Partei wählt und, wenn es angebracht ist, auf die richtigen Parolen hört: „Legal? Illegal? Egal!“ Vor dreißig Jahren hieß das letzte Wort aber noch anders.

---

# Warnung vor dem Microsoft Internet Explorer

Ich ärgere mich immer maßlos über den Quatsch, den Spiegel Online und andere Medien zum Thema Computersicherheit von sich geben.“Finger weg vom Internet Explorer – das empfiehlt das Bundesamt für Sicherheit in der Informationstechnik. Eine Sicherheitslücke ermöglicht es, Schadsoftware über den Browser einzuschleusen. Es genügt, infizierte Webseiten aufzurufen. Ein Sicherheitsupdate steht noch aus.“ Und was lesen wir bei Heise? „Da der Exploit dafür JavaScript verwendet, hilft es als temporäre Maßnahme, JavaScript zu deaktivieren.“ Welcher verblödete DAU surft denn mit eingeschaltetem Javascript auf unbekannte Websites? Davor warnt das Bundesamt für Sicherheit in der Informationstechnik schon seit Jahren. Vermutlich weiß man bei Spiegel online aber gar nicht, was Javascript ist oder wird, wie bei vielen Medien-Unternehmen, gewzungen, eine bestimmte kommerzielle Software zu benutzen. Selbst schuld und hört auf zu Jammern!