Neusprech

Herzlichen Glückwunsch an neusprech.org – das Blog hat verdient den Grimme-Preis erhalten. Der Glückwunsch geht auch and Udo Vetter und sein lawblog.

Du bist Anonymous

Grün-Rot für Vorratsdatenspeicherung

Das grün-rot regierte Baden-Württemberg will sich auf der Innenministerkonferenz am Mittwoch in Frankfurt am Main dafür

einsetzen, dass die Vorratsdatenspeicherung wieder eingeführt wird. (Heise)

Wer hat uns verraten? Grüne und Sozialdemokraten!

Leider ist Gema nicht verfügbar

Ein Artikel von mir bei Taz online: „Die Website der Gema wird derzeit von einer Cyber-Guerilla attackiert und ist nicht erreichbar. ‚Anonymous' ergreift damit Partei für Youtube."

Mao hat dich eingeladen, sein Freund zu sein

Freunde in Mandarin

Mao hat dich eingeladen, Sein Freund zu sein

„Mao hat dich eingeladen, sein Freund zu sein“ – ein Artikel von mir im neuen Medienmagazin Nitro über das chinesische Netzwerk Renren.

Uniform der Beamten des nationalen Cyber-Abwehrzentrums geleakt

Die offizielle Uniform der Beamten des nationalen Cyber-Abwehrzentrums ist geleakt. (via presseschauer)

Chinesen greifen das Pentagon

an, revisited

*Diesen Artikel schrieb ich hier am 04.09.2007. Untertitel: „Offenbarung statt Recherche.“ Das Niveau der Berichterstattung hat sich nicht geändert: Einer schreibt vom Anderen ab, ohne die Fakten zu überprüfen. Irgendwann ist die Zahnpasta aus der Tube und keiner will es gewesen sein. Die pöhsen Chinesen waren es so lange nicht, bis mir jemand Beweise zeigt, die **nicht** von Geheimdiensten oder anderen Pressure Groups mit einschlägigen Motiven stammen.*

Die Financial Times hat es behauptet und alle plappern es natürlich nach: „Chinese military hacked into Pentagon“. Jetzt stelle mer uns ganz dumm. Ist das wahr? Gibt es Beweise? Ist das möglich? Kann man das überprüfen?

Die Zeit ersetzt die Recherche durch Offenbarung: „Hacker des chinesischen Militärs sind offenbar ins EDV-Netzwerk des Pentagon vorgedrungen.“ Anschließend beruft man sich auf die *FTD*. „Wie die britische Zeitung am Dienstag unter Berufung auf amerikanische Regierungsstellen berichtete, wurden bei dem Hacker-Angriff auch Teile des EDV-Systems im Büro von US-Verteidigungsminister Robert Gates zum Absturz gebracht. Falls das so stimmt, bedeutet es, dass die Computerexperten Chinas inzwischen in der Lage sind, zentrale Systeme andere Länder stillzulegen.“

„Falls das so stimmt“ – ein journalistisches Armutszeugnis. Wenn man etwas nicht weiß, muss man es eben nachprüfen und nicht irgendwelche Gerüchte in die Welt hinausposaunen, nur weil es andere auch tun. Und was ist, wenn es nicht stimmt?

Nimmt die *Zeit* dann alles zurück und behauptet, es sei in Wahrheit Osama bin Laden gewesen? Und der Heise-Newsticker? „Chinesische Angreifer stecken offenbar hinter Cyber-Attacke auf das Pentagon“ Offenbar. Oder auch nicht.

Nach der Attacke Mitte Juni hatte das Pentagon 1500 Rechner für mehr als eine Woche offline genommen. Nun heißt es, auf dem erfolgreich angegriffenen Mail-Server hätten „größtenteils“ keine vertraulichen Daten gelegen. Momentan laufen noch Untersuchungen darüber, wie viele Daten entwendet wurden. Vor Kurzem gab es auch Berichte…“ Es gab Berichte.

Und was sagt uns das jetzt? Es gab auch Berichte, dass Hänsel und Gretel in den Wald gegangen seien. Man muss zugunsten des *Heise-Newtickers* anmerken, dass der nicht vorgaukelt, eigene Quellen zu besitzen oder selbst recherchiert zu haben. Nein, alles ist abgeschrieben. Was sagt also das Original?

„The Chinese military hacked into a Pentagon computer network in June in the most successful cyber attack on the US defence department, *say American officials*.

The Pentagon acknowledged shutting down part of a computer system serving the office of Robert Gates, defence secretary,

but *declined to say* who it believed was behind the attack.

Current and former officials have told the *Financial Times* an internal investigation has revealed that the incursion came from the People's Liberation Army.

One *senior US official said* the Pentagon had pinpointed the exact origins of the attack. *Another person familiar with the event said* there was a ‚very high level of confidence…trending towards total certainty' that the PLA was responsible."

Es ist also alles supergeheim, so supergeheim, dass eine Person, die mit dem Ereignis vertraut ist, es gleich ausplaudert. Der Rest nicht nur diesen Artikels, sondern auch aller, die von ihm abschreiben, ist gefüllt mit Textbausteinen über Merkels Besuch in China undsofort. hat also nichts damit zu tun. Der Kern ist ein Gerücht aus „gewöhnlich gut unterrichteten Kreisen." Um die Pointe gleich vorwegzunehmen: Die China-Hacker kommen nicht. Vielleicht bin ich ein notorischer Zweifler, Nörgler, Querulant, Besserwisser – aber ich glaube kein Wort. Das klingt so nach der Sprechblase: „Verfassungsschutz: Immer mehr Nazis nutzen das Internet."

Ganz einfach. Oder offenbar auch nicht: Wer einen Server angreift, sollte und könnte vielleicht vorher auf die Idee kommen, seine Spuren zu verbergen – etwa mit schlichten Mitteln wie mit einem Tor-Server. Sollte die Volksbefreiungsarmee Rechner des Pentagon angreifen, ohne

dafür zu sorgen, dass ihre IP-Adressen vorher geschreddert werden? Wikipedia wäre nicht auf dem neuesten Stand, dort ist von „veralteter Kommunikationstechnik“ in Chinas Streitkräften die Rede. Aber: „Allerdings wurden in der Miliz Einheiten geschaffen, die sich auf moderne Kommunikationstechnik spezialisieren und aus Bewohnern der urbanen Zentren des Landes rekrutieren. Diese Fachleute sollen ihr zivil erworbenes Wissen um die Computertechnik in die VBA einbringen.“ Da haben wir’s: Die Miliz war es. Und die hat „zehn Millionen Angehörige“. Dann kann Schäuble bald damit rechnen, selbst ständig online durchsucht zu werden.

Bilder: Hacker der Zhōnggúo Rénmín Jiěfàng Jūn bei einer Parade (oben). Der chinesische Hacker-Minister □□□□□□□/□□ □□□□□ (Mitte). Hacker der Volksbefreiungsarmee bereiten sich auf der Online-Durchsuchung von Second Life vor.

Cyberdings

„Die Dramatik des ‚Cyber-War‘ beruht keineswegs darauf, daß wir nun von so vielen bösen Chinesen und Russen angegriffen werden. Sie beruht darauf, daß wir selbst etwa 20 Jahre lang

in Ignoranz und Dummheit einen so großen Haufen schlechter IT-Technik aufgetürmt haben, der so voller Sicherheitslöcher ist, daß wir sie nicht mehr in den Griff bekommen – die schiere Quantität, aber auch das Fehlen einer eigenen Industrie in diesem Bereich machen das unmöglich. (…) Daß aber der Cyber-War und unsere Verletzlichkeit tatsächlich nur die Folge von über 20 Jahre politischer und wissenschaftlicher Ignoranz ist, und unser Sicherheitsproblem der in dieser Zeit als Infrastruktur aufgehäufte unsichere Mist, also nicht die bösen Hacker, sondern unser Management und unsere Politik die Täter sind, wird verschwiegen. Die Unsicherheit, die Verletzlichkeit im Cyber-War ist nicht systemimmanent. Sie ist eine spezifische Eigenschaft des IT-Mistes, aus dem wir in den letzten 20 Jahren unsere Infrastruktur kritiklos gebaut haben." (Hadmut Danisch, via Hal)

Nicht ich bin's gewesen, die Hacker sind es gewesen

Spiegel ~~online~~ im Interview mit Kasperksy („ein russisches Softwareunternehmen (…) hat sich auf die Entwicklung von Sicherheitssoftware spezialisiert"):

„So hält auch der Russe es für die wahrscheinlichste Erklärung, dass der Computerwurm Stuxnet, der im vergangenen Jahr viel Aufmerksamkeit auf sich zog, eine amerikanisch-israelische Erfindung sein könnte". Könnte? Hätte? Würde? Fakten? Fehlanzeige.

„Mutmaßlich über verseuchte USB-Sticks gelangte er in iranische Atomanlagen." Mutmaßlich? Seit wann verbeiten Journalisten Mutmaßungen und verschweigen sogar die Quelle der

Gerüchte? Stand es in der Bild-Zeitung?

„Aber selbst für den großen Stromausfall, der Teile Nordamerikas im August 2003 lahmlegte, macht Kasperski mittlerweile PC-Schädlinge verantwortlich“. Wer hätte das gedacht. Die Firma verkauft Software gegen „PC-Schädlinge“.

„Ich bin mir heute ziemlich sicher, dass diese Katastrophe von einem Virus ausgelöst wurde.“ Ich bin mir ziemlich sicher, dass Kaspersky das Interview benutzen will, um seine eigenen Produkte loszuwerden. Und ich bin mir ziemlich sicher, dass Kasperky wusste, dass deutsche Journalisten keinen kritischen Fragen stellen, wenn es um Computer und Internet geht, und auch an Fakten nicht besonders interessiert sind, nur an vagen Bedrohungsszenarien.

„Er will überdies nicht ausschließen, dass hinter vielen der aktuellen Hackerattacken heute Regierungen stecken.“ Ich will nicht ausschließen, dass ich mich bewerbe, Vorsitzender der Piratenpartei zu werden. Ich will auch nicht ausschließen, dass der Kaiser nackt ist und er gar keine neuen Kleider trägt.

„In Zukunft allerdings müssen wir mit Cyber-Attacken auf Fabriken, Flugzeuge und Kraftwerke rechnen.“ Nicht nur das: Auch mit Attacken auf harmlose kleine Privatrechner, die mit gaaaaanz vielen „Bundestrojanern“ nur so gespickt werden. Wie die Kollegin Annette Ramelsberger schon vor vielen Jahren schrieb: „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.“

„Kasperski zum SPIEGEL: ‚Alles, was wir erreichen können ist, zu verhindern, dass da draußen alles außer Kontrolle gerät.'“ Ja, genau! Kauft mehr „Anti-Viren-Programme“ von Kapersky! Das

Ende ist nahe!

You haben uns zu helfen

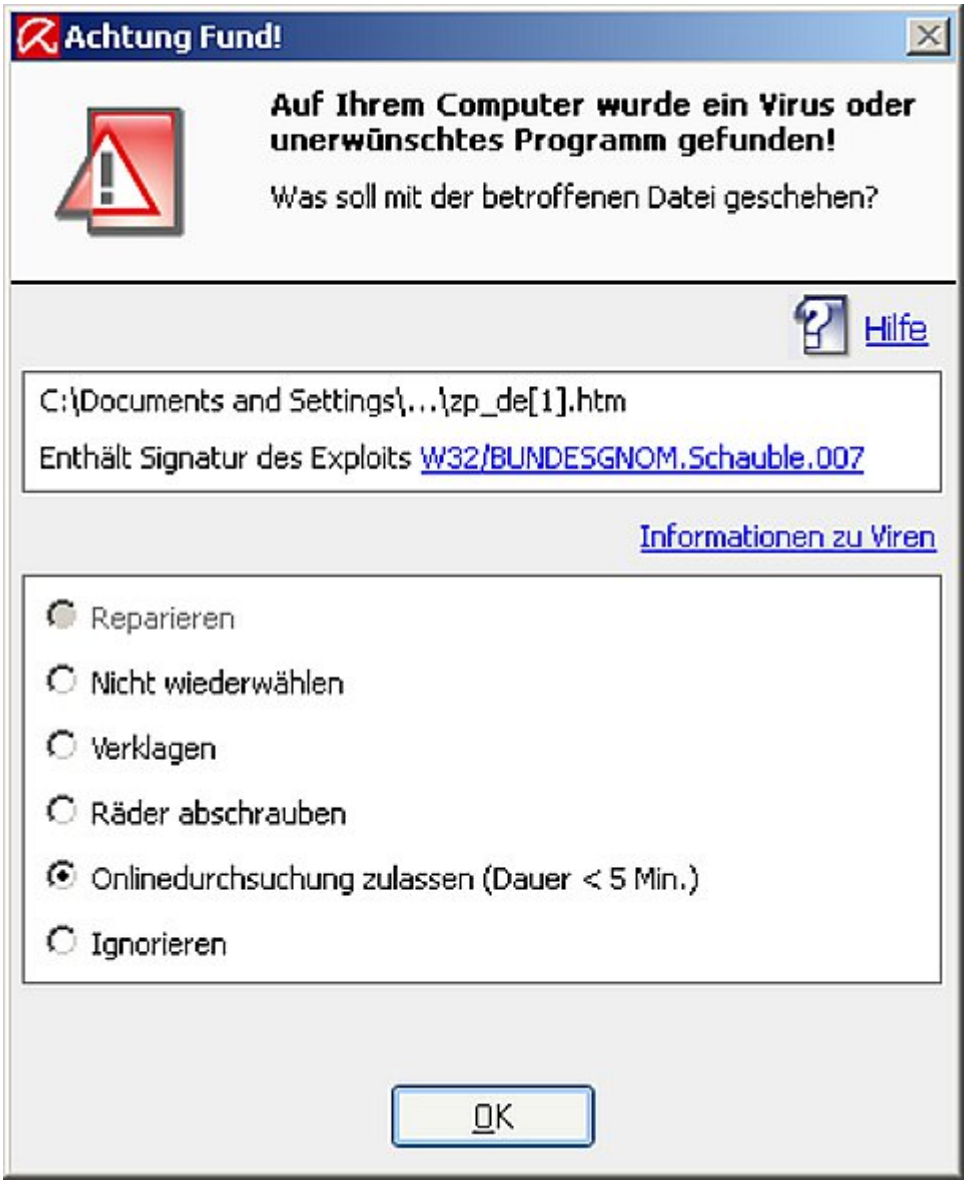
Achtung! Unsere geschätzten Webmail Benutzer
Wir haben gegenwärtig eine in-aktive Webmail-Konto sehr ähnlich wie diese wollen wir unverzüglich löschen.
Wir sind mit Problem zu wissen, welches es ist zu delete.You haben uns zu helfen, festzustellen, welches Konto ungültig ist die Überprüfung dieses Konto zu kaufen.
Um weiterhin mit dieser Webmail-Konto, müssen wir es sofort überprüfen, um nicht endgültig gelöscht.
Wenn Sie der Inhaber dieses Kontos sind und Sie sicher sind, es ist immer noch in Gebrauch ist, bitte Klicken Sie auf diesen Link, um zu überprüfen http://www.southshieldsfc.com/contactpage/use/form1/form1.html
Bitte, wenn der Link zur Zeit nicht verfügbar ist, schlagen Sie antworten Registerkarte Eingabeverifizierung hier und klicken Sie auf senden zur Abfrage sutmit Und ihr werdet umgehend eine Bestätigung, danke!
Warnung! Andernfalls wird es die in-aktives Konto und Ergebnis in den lockeren Ihres Kontos nicht übernommen werden.
Bitte beachten Sie: Sie können möglicherweise nicht in der nächsten Anmeldung andernfalls zu überprüfen.

Skriptum Internet-Recht

Skriptum Internet-Recht (pdf, 559 Seiten, Stand: April 2011) von Prof. Dr. Thomas Hoeren, Institut für Informations-, Telekommunikations- und Medienrecht, Universität Münster

---

Bundestrojaner Chop Suey, revisited



Die Bundesregierung macht keine Angaben dazu, ob sie den Bundestrojaner gegen Terrorverdächtige einsetzt hat. Wer hätte das gedacht! Geht ja auch nicht. Sie können ja nicht sagen: Heyy, wir haben es nicht hingekriegt, weil wir nicht wussten, wie wir die Software auf den Rechner des Verdächtigen hätten beamen sollen. Er hat uns leider nicht heimlich in seine Wohnung gelassen.

Es reicht doch aus, den Medien wie Golem die Verschwörungstheorie verbreiten, es gäbe eine „Online-Durchsuchung“ (aka Fernwartung eines Privatrechners durch Ermittlungsbeamte). By the way: der so genannte „Trojaner“ (der gar kein Trojaner ist, sondern eine ganz normale Spionagesoftware), schnüffelt per Skype. **Das ist etwas anderes!**

Sächsisches Staatsministerium des Inneren abgemahnt

Eine Kölner Kanzlei mahnt das Sächsische Staatsministerium des Inneren ab:

„Am 8. Juni 2011 beschlagnahmten Beamten der Integrierten Ermittlungseinheit Sachsen (INES) die Server von kino.to und veröffentlichten unter der URL www.kinto.to [sic] folgenden Hinweis:

„Die Kriminalpolizei weist auf Folgendes hin:
Die Domain zur von Ihnen ausgewählten Webseite wurde wegen des Verdachts der Bildung einer kriminellen Vereinigung zur gewerbsmäßigen Begehung von Urheberrechtsverletzungen geschlossen. Mehrere Betreiber von KINO.TO wurden festgenommen.

Internetnutzer, die widerrechtlich Raubkopien von Filmwerken hergestellt oder vertrieben haben, müssen mit einer strafrechtlichen Verfolgung rechnen.“

Damit sind Sie als Dienstherr der Kriminalpolizei Sachsen gem. § 2 Nr. 1 Telemediengesetz Diensteanbieter und müssen den im Telemediengesetz vorgeschriebenen Informationspflichten nachkommen. Dies haben Sie ganz offensichtlich versäumt. § 5 Telemediengesetz schreibt nämlich vor, dass jede Internetseite ein Impressum vorhalten muss.“

Bruhahahaha.

Richtig und falsch reinhacken

Richtig bei Heise Security: „Bei dem Diebstahl von rund 200.000 Kundendaten der Citibank mussten die Kriminellen nicht tief in die Trickkiste greifen, wie ein Sicherheitsexperte gegenüber der New York Times bekannt gegeben hat. Demnach gelang der unberechtigte Zugriff, den die US-Bank bei einer Routinekontrolle Anfang März entdeckt hat, durch das simple Manipulieren eines URL-Parameters.“

The method is seemingly simple, but the fact that the thieves knew to focus on this particular vulnerability marks the Citigroup attack as especially ingenious, security experts said.

Falsch bei Spiegel ~~online~~: „Den beiden Angeklagten wird vorgeworfen, zwischen März 2009 und März 2011 Computer von Musikfirmen manipuliert zu haben. Mit Spionageprogrammen, sogenannten Trojanern, stahlen sie laut Anklage bis dahin unbekannte Songs…“

Wer schützt unsere Kinder eigentlich vor den Verschwörungstheorien der Holzmedien, zu denen auch gedrucktes linkfreies Papier à la Spiegel ~~online~~ gehört? Lugt da wieder die real gar nicht existierende „Online-Durchsuchung“ hervor? Guckst du hier:

Spiegel Online (ein Link zur Quelle, o Wunder!) fantasiert wieder wahllos herum: „Denn Bronk hackte sich in deren E-Mail-Konten…“ Das hätte die Taz auch nicht schlechter formulieren können. Wie zum Teufel, „hackt“ man sich in E-Mail-Konten? Etwa mit einer real gar nicht existierenden „Online-Durchsuchung“?

Nein, der Kerl war kein echter „Hacker“, sonder jemand, der sich des guten alten Social Engineering bediente: „Ausgestattet mit dem derart zusammengetragenen Hintergrundwissen ging er daran, die E-Mail-Passwörter seiner Opfer zu ändern. Dazu machte er sich nicht etwa die Mühe, zuerst deren Passwort herauszufinden. Stattdessen gab er sich deren E-Mail-Providern gegenüber als Inhaber des jeweiligen Accounts aus und beantragte, mit der Begründung, er habe sein Passwort vergessen, online ein neues. Weil viele Provider immer noch Standardabfragen, beispielsweise nach dem Mädchennamen der Mutter, verwenden, um in solchen Fällen die Identität des Antragstellers zu überprüfen, fiel es Bronk nicht schwer, die E-Mail-Konten zu übernehmen.“

„Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.“

Also bitte keine Computermythologie, Technik-Schamanismus oder

anderen Regenzauber: Man kann sich nicht einfach so irgendwo „reinhacken“.

Isharegossip, revisited

„Auf der Website isharegossip.net heißt es, die Domain isharegossip.com sei gestohlen worden.“ (Wer es nicht glaubt: Es steht so bei Heise).

Foren-Nutzer wissen mehr: „Die MX records wurden geändert auf plsmtp2.hushmail.com und plsmtp1.hushmail.com. Damit dürfte es zumindest in den ersten Stunden möglich gewesen sein, ’ne Menge eMails abzugreifen.“

Der wahre Wert von Facebook

Phishing-Angriff auf den Internationalen Währungsfonds

Ein Leserkommentar im Heise-Forum: „Wenn eine Firma oder Institution, erst recht, wenn diese mit sensiblen Daten zu tun hat, ihre Mitarbeiter nicht halbwegs zu schulen in der Lage ist, wie man mit solchen Mails umzugehen und dass man eben nicht wahllos auf Links zu klicken hat … sorry, dann hat sie es einfach nicht anders verdient als ausspioniert zu werden. Vermutlich findet man in den Papiermüll-Containern hinterm Haus auch massenhaft Akten in einwandfreiem Zustand inkl. Stempel ‚Streng geheim!'"

Ich finde, dass man eine Firma, die keine vernünftige E-Mail-Policy hat, deren Mitarbeiter noch nicht einmal mit Javascript umgehen können und die so doof sind, dass sie auf Phishing hereinfallen, sogar noch Strafe zahlen müsste.

Whois abschaffen!

Ein lesens- und erwägenswerter Kommentar Lutz Donnerhackes bei Heise: „Warum die Datenbank illegal und nutzlos ist“.

„Nur weil Techniker es ursprünglich als nützlich empfanden, ihre privaten Adressbücher gegenseitig abfragbar zu machen, muss diese Praxis nicht durch Rechteverwerter und Strafverfolgungsbehörden als zentrale Grundkomponente des Internets angesehen werden. (…) Die Datensammlungen des Whois entbehren formaler internationaler Grundlagen, sie stehen im direkten Widerspruch zu nationalen Gesetzgebungen. Der deutsche Datenschutz beispielsweise verbietet direkt die Erhebung der Daten, da kein konkreter Verwendungszweck vorliegt. (…) Die Daten im Whois sind für den Verwendungszweck der Strafverfolgung wertlos. (…) Möglicherweise ist der Whois-Dienst generell einzustellen.“

E-Mail-Schreiben ist nicht schwer

Von: presse@jugendkulturen.de
Antwort an: presse@jugendkulturen.de
Datum: 09.06.2011 18:11
An: Burkhard Schröder <burks@burks.de>

09. Juni 2011

[if gte mso 9]><xml> <w:WordDocument> <w:View>Normal</w:
<w:SaveIfXMLInvalid>false</w:SaveIfXMLInvalid> <w:IgnoreMi
<w:BreakWrappedTables/> <w:SnapToGridInCell/> <w:WrapTe
<w:BrowserLevel>MicrosoftInternetExplorer4</w:BrowserLevel>
</w:LatentStyles></xml><![endif]<!-- /* Font Definitions */
4;mso-font-charset:0;mso-generic-font-family:swiss;mso-font
6 4 3 5 4 4 2 4;mso-font-charset:0;mso-generic-font-family:
div.MsoNormal{mso-style-parent:"";margin:0cm;margin-bottom:
Roman";}a:link, span.MsoHyperlink{color:blue;text-decoratio
span.MsoHyperlinkFollowed{color:purple;text-decoration:unde
Section1{size:612.0pt 792.0pt;margin:70.85pt 70.85pt 2.0cm
mso 10]><style> /* Style Definitions */ table.MsoNormalTabl
Tabelle";mso-tstyle-rowband-size:0;mso-tstyle-colband-size:
5.4pt;mso-para-margin:0cm;mso-para-margin-bottom:.0001pt;ms
Roman";mso-ansi-language:#0400;mso-fareast-language:#0400;m

Sehr geehrte KollegInnen und Kollegen in den Medien,

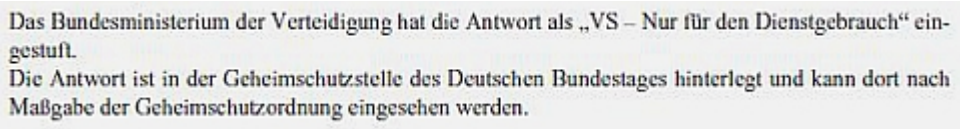
wir möchten Sie herzlich einladen, das Projekt Zeitmaschine

Seit April 2011 arbeitet das Archiv der Jugendkulturen mit
ältere Menschen zu verschiedenen Ereignissen aus der Vergan
stellen diese Daten zu multimedialen Clipszusammen. Die Cli

dot.gif verein_klein.jpg

… doch manche lernen’s nimmer mehr. Das kommt davon, wenn man Word benutzt und E-Mails auch noch in HTML verfasst.

Geheimschutzstelle


Das Bundesministerium der Verteidigung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Digitale Linke: „Bundesregierung begründet neue Geheimhaltungspflichten mit dem Internet (…)

Die Bundesregierung sieht neue Geheimhaltungsnotwendigkeiten wegen der Möglichkeiten digitaler Technologien. (…) Die Antwort (