Der Bundestrojaner

E.R. Sexauer

26.Oct.2007

Zusammenfassung

Seit Monaten geistert der Bundestrojaner oder die sogenannte heimliche Onlinedurchsuchung durch die Presse. Wenn man dem Minister Schäuble glauben darf, flehen ihn die Ermittlungsbehörden ständig an, dieses Verfahren legal zu machen. Im folgenden wird untersucht, welche technischen Möglichkeiten zum Einpflanzen des Spions es überhaupt gibt und wie man sich dagegen wehren kann.

1 Zielsetzung

Laut Bundesschäuble soll es der Trojaner[1] ermöglichen, beliebige Systeme anzugreifen und ohne Kenntnis des Besitzers auszuspionieren. Die dazu verwendeten Methoden sollen existieren und sind natürlich streng geheim. Wenn das Gesetz durch ist, soll es in Deutschland verboten werden, über die dabei verwendete Technik zu publizieren - oh welche Weisheit!

1.1 Zur Terminologie

Auch wenn man von 'dem Bundestrojaner' spricht, handelt es sich nicht um EIN Programm im gewöhnlichen Sinne. Es geht vielmehr um ein Konzept und einen dazugehörigen Satz von Werkzeugen. Im Anwendungsfall müssen diese Werkzeuge individuell an das Betriebssystem und die Software des Opfers angepaßt werden. Um mit der Entwicklung von Betriebssystemen und Schutzsoftware Schritt zu halten, sind kontinuierliche Programmierarbeiten erforderlich.

1.2 Ein rechtlicher Aspekt

Wenn eine Privatperson gängigen Systemen soviel Unsicherheit bescheinigen würde, daß sie jederzeit gehackt werden könnten, müßte er das entweder beweisen oder sich mit saftigen Klagen der Hersteller auseinandersetzen. Schäuble

[1] Die technisch genaue Unterscheidung zwischen Viren, Würmern und anderem Getier ist in diesem Zusammenhang nicht erforderlich. Der allgemeine Begriff Schadsoftware reicht aus.

beweist nichts; er hat es ja nicht nötig. Hinter Geheimhaltung kann man sich trefflich verstecken.

1.3 Die Zielobjekte

Laut Schäuble sind dies gefährliche Kriminelle wie Rauschgifthändler und Terroristen. Natürlich soll das Verfahren nur bei dringendem Verdacht eingesetzt werden und rechtlich abgesichert sein...

1.4 Das Zielsystem

Zielsysteme sind marktübliche PC's, die über einen DSL-Anschluß mit dem Internet verbunden sind. Rechtlich und technisch ist es schon heute möglich, den Datenverkehr auf solchen Leitungen unbemerkt aufzuzeichnen und sich unbemerkt einzuschalten[2].

Der Bundesschäuble will aber mehr; er will über diese Leitung unbemerkt Schadprogramme einpflanzen, die es ihm erlauben das Zielsystem zu erkunden - lies Platte durchsuchen und Ein- Ausgabe aufzeichnen.

1.5 Voraussetzungen für einen Angriff

Ein vernünftig konfiguriertes System[3] kann nur angegriffen werden, wenn im Betriebssystem oder in einem der verwendeten Anwendungsprogramme Fehler sind. Diese Fehler müssen dem Angreifer bekannt sein und das Opfer muß die fehlerhaften Programmteile tatsächlich benutzen.

- Eine einfache Variante ist es, dem Opfer vergiftete Mails oder Webseiten vorzusetzen. Allerdings müßte das Opfer dann so hilfsbereit sein, diese vergifteten Teile tatsächlich zu laden.
- Eine etwas bessere Variante besteht darin, in Mails oder Webinhalte, die das Opfer anwählt, vergiftete Teile so einzubauen, daß das Opfer dies nicht merkt. Beispiel: Das Opfer wählt 'spiegel.de' mit einem Bild des Bundesschäubles an. Anstelle des Originalbildes blendet der Angreifer ein äußerlich ähnliches, aber vergiftetes Bild ein.
- Die brutale Variante besteht darin, unbemerkt beim Opfer einzubrechen und den Spion manuell auf seiner Maschine zu installieren.

[2] 'Man in the middle' lautet der technische Fachausdruck dafür. Dieser böse Mann versucht beiden Seiten vorzumachen, er sei jeweils der andere.

[3] Vernünftig konfiguriert heißt in diesem Fall, daß das System eingehende Daten nur dann akzeptiert, wenn diese als Antwort auf eine eigene Anfragen kommen. Das ist heute marktüblich. Wirklich gute Systeme kontrollieren auch den ausgehenden Datenverkehr. Das ist leider (noch) nicht marktüblich.

Voraussetzung ist in beiden ersten Fällen, daß der Browser oder Mailclient tatsächlich die vom Angreifer vermuteten Fehler hat und daß das - wie Herr Schäuble glaubt - ahnungslose Opfer, diese fehlerhaften Programme zum Zeitpunkt des Angriffs tatsächlich auch verwendet. Im dritten Fall darf das Opfer nicht merken, daß sein PC angefaßt wurde.

1.6 Der Spion ist im System

Nehmen wir mal an, der Spion hat sich tatsächlich vom Opfer unbemerkt im System eigenistet. Jetzt gilt es, noch einige weitere Klippen zu umschiffen:

1.6.1 Neustart des Systems

Der Spion muß sich auf der Festplatte niederlassen und beim Systemstart unbemerkt aktiviert werden. Alternativ müßte er bei jeder Internetverbindung neu eingeschleust werden.

1.6.2 Sicherheitssoftware

Im technischen Sinne ist der Spion ein Schadprogramm. Sicherheitstools wie Virenscanner, Intrusiondetctors und ähnliche sind dazu konstruiert, unerwünschte Eindringlinge zu erkennen und zu bekämpfen. Wenn es dem Bundesschäuble nicht gelingt, die Hersteller dieser Programme zur Kooperation zu bewegen, ist die Entdeckungsgefahr groß. Wenn es ihm gelingen sollte, wird sich das nicht lange geheim halten lassen.

Da viele Hersteller von Schutzsoftware im - aus Schäubles Sicht - feindlichen Ausland sitzen, wird er diese kaum zwingen können, ihre Produkte gegen den Bundestrojaner blind zu machen.

1.6.3 Wie sendet der Spion?

Ein Spion ist nur nützlich, wenn er seine Daten unbemerkt an den Auftraggeber senden kann. Zumindest bei Linux ist es nicht schwer, die Protokollierung des ausgehenden Datenverkehrs zu erzwingen. Da es dazu eine Vielzahl alternativer Methoden gibt, müßte der Trojaner erstmal herausfinden, ob es solche Schutzmaßnahmen gibt und wie diese arbeiten. Als nächstes müßte er diese abschalten, ohne daß sein Opfer dies bemerkt. Nicht trivial.

Natürlich könnte es auch bei Windows solche Schutzmaßnahmen geben, wenn sich der Hersteller mehr mit der Sicherheit seines Systems beschäftigen und die erforderlichen Hilfsmittel mitliefern würde[4].

[4] Das wäre übrigens auch eine gute Schutzmaßnahme gegen vom Eigentümer unbemerkten Spamversand.

1.7 Wie sendet das Opfer?

Wie schon bemerkt, kann die DSL-Leitung unbemerkt abgehört werden. Dieses Abhören hilft allerdings bei verschlüsseltem Datenverkehr - SSH, Https oder TLS - nichts[5]. Dann kann nur festgestellt werden, wohin gesendet wurde; der Inhalt selbst kann nicht entschlüsselt werden, es sei denn der Trojaner hat unbemerkt vollen Zugriff auf die Maschine; in diesem Fall könnte er Zertifikate auslesen und Tastatureingaben mitschneiden.

2 Wie wehrt sich das Opfer?

In den oben geschilderten Szenarien wird sich das Opfer keineswegs so ahnungslos verhalten, wie es der Bundesschäuble offenbar annimmt. Die Zielgruppe besteht ja angeblich aus Hochkriminellen die weder ahnungslos noch zu arm sind, um sich entsprechendes Knowhow einzukaufen.

2.1 Einfach und wirksam

Kaum eine Drogenhändler wird so dumm sein, seine Ware vom heimischen PC aus übers Internet zu bestellen - womöglich noch im Klartext. Wenn schon Internet, wird er die paar Euro ausgeben, mit denen er anonym im Internetcafe surfen kann.

2.2 Etwas komplizierter

Wenn er schon nicht auf die Bequemlichkeit des heimischen PC's verzichten will, wird er sein System von CD aus booten - dort können sich keine Trojaner festsetzen. Natürlich wird er mit diesem System auch nichts anderes machen.

2.3 Serverlösung, ganz professionell

Prinzipiell ist es problematisch, wenn sich ein Rechner auf dem angreifbare Anwendungen laufen, selbst schützen soll. Je nach Rechten, die sich ein potentieller Eindringling im System erschleicht, kann er ja die Schutzmaßnahmen erspähen und sabotieren. So wäre es z.B. ein Riesenerfolg für den Angreifer, wenn es ihm gelänge, das Logging (Aufzeichnen von Systemereignissen) einzuschränken oder gar zu unterbinden.

[5] Genauer gesagt müssen die beiderseitigen Opfer einmal über einen sicheren Kanal Fingerabdrücke oder Zertifikate ausgetauscht haben. Damit kann der 'man-in-the-middle' erkannt werden. Den Fingerabdruck für den SSH-Hostkey kann man auch so nachprüfen; allerdings erst, nachdem man sich eingelogt hat.

In der Welt der Profis gibt es eine zuverlässige Methode, sein System zu schützen: Das Opfer betreibt zwei Rechner, eine Arbeitsstation und einen vorgeschalteten Server, über welchen die Internetverbindung und nur diese läuft; natürlich hat der Server ein eigenes Passwort. Selbst wenn der Angreifer volle Systemrechte auf dem Arbeitsplatzrechner erobern würde, käme er immer noch nicht an den Server heran. Insbesondere könnte der Server immer noch verhindern, daß der Angreifer seine Daten unbemerkt senden kann.

Der Server muß übrigens nicht über besondere Ressourcen verfügen. Eine alte Maschine, die untätig in der Ecke steht, tut es völlig.

2.4 Vereinfachte Serverlösung

Auch wenn das Opfer über nur einen Rechner verfügt, kann es darauf eine Serverlösung betreiben, indem es einen virtuellen Server (Vserver) installiert.

Ein Vserver besteht aus folgenden Komponenten:

- Der Host (Gastgeber). Aus Sicherheitsgründen empfiehlt sich hier eine Linux-Maschine.
- Eine Virtualisierungssoftware, die auf dem Host läuft; z.B. Vmware.
- Ein oder mehrere Gastbetriebssysteme, die auch gleichzeitig laufen können. Die Virtualisierungssoftware bietet dem Gastsystem eine virtuelle Maschine, die logisch wie ein eigener Rechner aussieht. Das Gastsystem nutzt zwar die Ressourcen des Hosts, hat aber auf diesen keinen direkten Zugriff. Natürlich hat das Gastsystem auch eigene Passwörter.

Die Sicherheitsregeln, die den Internetverkehr kontrollieren, laufen auf dem Host und sind von den Gastsystemen her nicht beeinflußbar. Natürlich sind auch die einzelnen Gastsysteme gegeneinander abgeschottet - auch wenn sie gleichzeitig laufen. So kann man sich beispielsweise einen Windows-Virus einfangen, ohne daß dieser ein parallel laufendes Linux stört.

Hardwareabhängige Hacks haben übrigens auf einem Vserver ein schweres Leben, da der Vserver dem Gastsystem nur logische Treiber anbietet; von der tatsächlich existierenden Hardware erfährt das Gastsystem nichts.

2.5 Manchmal ist weniger mehr

Wenn man auf graphische Werkzeuge verzichtet und die klassischen textorientierten Tools verwendet, entfallen viele mögliche Einbruchspunkte.

2.6 Schutz gegen Einbruch

Prinzipiell gibt es zwei Methoden:

- Man läßt den PC durchlaufen und sendet regelmäßig Lebenszeichen an einen externen Server. Damit fällt jede Unterbrechung durch Neustart auf.
- Man schaltet die Maschine aus und verklebt Stromschalter und Gehäuseschrauben mit einer im Handel erhältlichen, individuell markierten Folie. Damit fällt jedes Anschalten auf.

In beiden Fällen wird man das BIOS durch ein Passwort absichern. (Ob es die früher häufig vorhandenen, fest eingebauten Bios-Passwörter noch gibt, ist unbekannt. Auf jeden Fall sollte man sich nicht darauf verlassen, daß es sie nicht gibt. Wenn es sie noch gibt, dürfte es den Nachrichtendiensten nicht schwerfallen, sie zu erhalten.)

2.7 Genereller Schutz

Kritische Daten speichert man auf einem verschlüsselten Dateisystem. Auch ein Usb-Stick zur externen Speicherung kritischer Daten leistet gute Dienste - natürlich auch verschlüsselt.

2.8 Außer Reichweite

Eine kriminelle Organisation wird sich für wenig Geld einen Server in China oder einem anderen Land, das garantiert nicht mit dem Bundesschäuble kooperieren wird, mieten. Diesen kann man mit sicherer Verschlüsselung anwählen, um seine Kommunikation von dort aus zu betreiben.

Dann hat es sich ausgeschäublet.

3 Ein moralischer Aspekt

Natürlich fehlt es von der Regierungsseite nicht an den üblichen Argumenten:

- Anständige Bürger haben nichts zu verbergen und brauchen sich folglich nicht fürchten.
- Anständige Bürger unterstützen jede Bekämpfung der Kriminalität. Damit wird implizit unterstellt, Gegner der Onlinedurchsduchung unterstützten die Kriminalität.

Solche 'Argumente' wurden schon immer zur Unterwühlung des Rechtsstaats verwendet und werden durch Wiederholung nicht wirklich besser.

Natürlich werden auch die Erfolgsaussichten des Unternehmens dadurch nicht besser - im Gegenteil: Wenn man versucht, seine Kritiker auf solch unlautere Weise in die moralische Ecke zu stellen, zerstört man auch letzten Rest von Verständnis, der ursprünglich bei ihnen vorhanden gewesen sein mag.

Tatsächlich sind auch viele Gegner der Onlinedurchsuchung durchaus für harte Maßnahmen gegen Terroristen und Drogenhändlern. Ihre Kritik richtet sich gegen die erkennbare Nutzlosigkeit des Unternehmens.

4 Wie gut sind Schäubles Hacker?

Auch wenn Schäubles Hacker in ihrem subjektiven Glauben einer guten Sache dienen und formalrechtlich abgesichert sind, stehen sie faktisch auf Seiten derer, die zur Unsicherheit des Internets beitragen - und sei es nur durch Nichtpublikation von erkannten Sicherheitslücken. Wie sie das mit ihrem Berufsethos vereinbaren, ist natürlich ihre persönliche Entscheidung.

Zwangsläufig geraten sie durch ihrer Tätigkeit in Gegnerschaft zu den Leuten, die für die Sicherheit des Internets arbeiten und nicht bereit sind, auch nur einen Teil dieser Sicherheit für ein so fragwürdiges Unternehmen zu opfern.

Damit stehen Schäuble und ihre Kollegen in Sicherheitsdiensten anderer Länder gegen eine mächtige Gruppe internationaler Experten, die geographisch und weltanschaulich größtenteils außerhalbs Schäubles Reichweite liegt. Ob die Hacker es mit dieser Gruppe aufnehmen können, ist zweifelhaft. Ebenso zweifelhaft ist die Möglichkeit der Geheimhaltung. Von einem eventuellen Publikationsverbot in Deutschland werden sich die Sicherheitsexperten natürlich nicht abschrecken lassen...

Grundsätzlich problematisch ist der Angriff gegen Opensource-Systeme wie Linux oder BSD. Von dieser Community ist mit Sicherheit keine Tolerierung irgendwelcher Sicherheitslücken zu erwarten.

Auch wenn die Regierung über große finanziellen Ressourcen verfügt, ist sie schon rein numerisch gegen die Sicherheitsexperten in einer schlechten Position.

Leider ist das parlamentarische System in Deutschland schon so weit unterhöhlt, daß die Regierung hier unkontrolliert im Dunkeln operieren kann.

5 Der S+Dealer

Natürlich werden nicht alle Kriminellen gegenüber dem Bundesschäuble eine so negative Haltung einnehmen wie der Verfasser. Ein S+Dealer (Schäuble-positiv) wird sich ganz anders verhalten:

- Er benutzt Windows auf seinem Privatrechner für den Drogenhandel; von Sicherheitsupdates, Virenscannern und Intrusiondetectors hält er nichts. Wenn er sie überhaupt installiert, aktualisiert er sie nicht regelmäßig. Sicherheitsmeldungen ignoriert er grundsätzlich.
- Er ist ständig online und die bei Windows mitgelieferten Sicherheitstools reichen ihm aus - schließlich hat er für das System ja teuer bezahlt.
- Seine Dateien legt er im Klartext auf der Festplatte ab.
- Wenn er überhaupt externe Datenträger verwendet, legt er diese säuberlich beschriftet neben seinen Rechner.
- Mails und Links auf Webseiten, die ihm angeboten werden, öffnet er grundsätzlich - natürlich mit den vom Hersteller zu diesem Zweck gelieferten Programmen; er hat sie ja bezahlt, also werden sie auch genutzt.
- Von preisgünstigen Vservern im Internet hat er noch nichts gehört.

Diesen S+Dealer wird der Bundesschäuble vielleicht fangen. Allerdings fragt man sich, warum der S+Dealer sich nicht gleich selbst anzeigt...

6 Zusammenfassung

Die Zielgruppe, um die es angeblich geht, kann sich einfach und billig gegen den Bundesschäuble schützen. Wenn man damit überhaupt jemanden fängt, so sind es nur die Dummen, die man wahrscheinlich auch ohne Onlineüberwachung gefaßt hätte.

Unerwünschter Nebeneffekt:

Durch die öffentliche Debatte über den Bundestrojaner ist das Sicherheitsbewußtsein auch der Kriminellen natürlich gestärkt worden. Selbst wenn es bisher ein paar Leichtsinnskandidaten unter ihnen gegeben hat, die man vielleicht hätte fangen können, sind sie jetzt gewarnt und werden sich in Zukunft schützen - die Mittel dazu haben sie ja.

Good bye Schäuble.

7 Die Vertrauenskrise

Ein Aspekt, der den Bundesschäuble offenbar wenig interessiert, ist das Vertrauen in unsere angeblichen Beschützer.

- Das BSI (Bundesamt für Computersicherheit) galt bisher als seriöse Referenz in Sachen Sicherheit. Z.B. hat dieses Amt schon 'Sicherheits-CD's für Bürger' angeboten. Allerdings untersteht das BSI dem Innenministerium. Ob und inwieweit Sicherheitsvorschläge des BSI so reduziert werden, daß sie Maßnahmen gegen den Bundestrojaner ausklammern, sei dahingestellt; Gegenmaßnahmen wird es wohl kaum publizieren. Wirklich vertrauen kann man dieser Behörde allerdings nicht mehr. Ihre Sicherheits-CD will man vielleicht auch nicht mehr benutzen.

- Publikation und Behebung von Programmfehlern war bisher ein öffentlich diskutiertes Thema. Es gibt allerdings angeblich im Internet Börsen, auf denen man Beschreibungen nicht publizierter Fehler kaufen kann. Ob und in welchem Umfang die Bundesregierung solche fragwürdigen - letztlich kriminellen - Quellen nutzen will, ist unbekannt.

- Es wurde schon diskutiert, Sicherheitssoftware per Gesetz zur Nichterkennung des Bundestrojaners einzuschränken. Hersteller wie z.B. Kasperski, haben das rigoros angelehnt. Zum Glück (für uns) sitzen viele Hersteller im Ausland. Ob deutsche Hersteller sich erfolgreich gegen ein solches Gesetz wehren können, ist derzeit ungewiß. Ein böser Seiteneffekt wäre es dabei, daß durch solche Maßnahmen auch der Schutz gegen echte Schadsoftware eingeschränkt würde. Das Vertrauen zu den einheimischen Herstellern würde durch solche Gesetze in jedem Fall drastisch sinken.

- Noch toller ist die Idee, die Hersteller zu zwingen, den Bundestrojaner in ihre Produkte gleich mit einzubauen.

- Das Verbot technischer Publikationen in Deutschland ist ein Schildbürgerstreich, der begründete Zweifel am Verstand seiner Urheber aufkommen läßt. Schließlich weiß heute jedes Schulkind, wie man das umgeht.

- Eigentlich sollte man ja annehmen, daß solche Fragen im Parlament diskutiert werden. Uneigentlich werden sie es faktisch nicht.

Es versteht sich von selbst, daß das Vertrauen der Bürger zu ihren Beschützern durch solche teuren und erkennbar wirkungslosen Pläne erheblich beeinträchtigt wird.

Ein konkreter Fall

Anfag November-2007 berichtete die Presse über einen Fall. der die Problematik deutlich beleuchtet. Ein Hacker wurde festgenommen, dem man vorarf 250.000 Windows-PC's verseucht zu haben. Pikanterweise war dieser Mann Mitarbeiter einer Firma für Compuersicherheit. Gegenstand dieser Firma ist es, nichtveröffentlichete Sicherheitslücken in Betriebssystem und Anwendungen meistbietend zu versteigern.

In den Webseiten dieser ehrenwerten Firma kann man nachlesen, daß die Bieter streng auf Seriösität geprüft werden und daß dies alles zu unserem Besten ist, da die Entdecker der Sicherheitslücken auf diese Weise für ihre Arbeit entlohnt werden und in Zukunft umso eifriger nach Sicherheitslücken suchen werden.

Es mag sein, daß solche Geschäfte formaljuristisch sogar legitim sind. Dubiös sind sie trotzdem. Ein genauer Blick auf die angebotenen Exploits zeigt, daß mögliche Angriffe auf Privatrechner am höchsten im Kurs stehen. Das ist genau die Zielgruppe des Bundestrojaners.

Eigentlich sollte man ja vom BSI erwarten, gegen solche dubiosen Praktiken vorzugehen. Schließlich wird diese teure Behörde aus öffentlichen Geldern finanziert und hat den Auftrag, uns gegen Softwarepiraten zu schützen.

Uneigentlich untersteht das BSI aber dem Bundesschäuble, dessen Onlineschnüffler aus genau diesen Quellen schöpfen. Auch wenn er nicht wahrhaben will, er spielt mit diesen obskuren Geschäftemachern in der gleichen Liga.

Was wird das BSI also in solchen Konfliktfällen tun? Die Antwort ist einfach: Es wird das tun, was Beamte schon immer getan haben. Es wird sich auf Dienstvorschriften und Gehorsam berufen und seine Hände in Unschuld waschen. Der Schutz der Bürger bleibt dabei auf der Strecke.

Wer eigentlich schützt uns vor unseren Beschützern???

8 Das Wie verstehe ich, aber nicht das Warum

Falls der Bundesschäuble überhaupt mit seinen Experten diskutiert, weiß er alles oben Gesagte auch. Warum dann dieser sinnlose und teure Aktivismus? Es gibt zwei Antworten, die sich logisch ergänzen:

- Schäuble ist ein Politiker, der sich profilieren und wiedergewählt werden will. Er verläßt sich darauf, daß die Mehrzahl seiner Kollegen und Wähler die Technik nicht verstehen und ihm und den von ihm vorgeschobenen Experten glauben. Man muß nur lange genug über einen beliebigen Begriff reden, bis einige tatsächlich an die Existenz des Gegenstands glauben.
- Auch wenn diese Maßnahme wirkungslos sein wird, ist sie ein erster Schritt zu weitergehenden Gesetzen. Damit kann man das Thema noch jahrelang am Kochen halten.

Daß ausländische Politiker ins gleiche Horn tuten und damit scheinbar Schäubles Konzept bestätigen, ist nicht verwunderlich. Schließlich sind sie auch Politiker und handeln aus den gleichen Motiven. Österreich beruft sich auf Deutschland und Deutschland beruft sich auf Österreich. 'Fuck-yourself-theorie' nennen die

Amerikaner das unfein, aber treffend. Man kann es leider nicht ausschließen, daß es dadurch in den Augen dieser Politiker wahrer wird...

Welch eine schöne Gelegenheit, eine neue Behörde zu schaffen. Daß sie nutzlos sein wird, stört den Politiker Schäuble nicht; er muß sie ja nicht bezahlen; das tut der kleine Mann auf der Straße.

Das Problem ist nicht, daß der Bundesschäuble zu dumm ist, um zu verstehen, was er da macht. Damit könnte man zur Not noch leben. Das wahre Problem ist, daß er ein berechnender Politiker ist, der weiß, daß er damit durchkommen wird und daß seine Kollegen, die genauso handeln, ihn decken werden - egal wieviel Geld er mit dieser sinnlosen Aktion verschwenden wird. Die Bürger zahlen ja; sie haben es schon lange verlernt, zu protestieren.

Das Ministerium hat verlauten lassen, daß die Entwicklung des Trojaners rund 200.000 Euro kosten wird und zwei Programmierer erfordet - zusätzlich und permanent, darf man annehmen[6]. Eventuelle Mehrkosten werden natürlich völlig unvorherbar und keinesfalls durch den Minister zu vertreten sein...

Daß die Regierung es wagt, uns eine so plumpe und dreiste Lüge aufzutischen, bezeugt ihre Geringschätzung der Bürger. Es ist übrigens die gleiche Regierung, die zig-Million Euro braucht, um ein paar Webseiten zu erstellen. Es ist auch die gleiche Regierung, die den Vertrauensschwund zur Politik und deren Repräsentanten beklagt.

Das Parlament, das die Regierung ja angeblich beaufsichtigt, schweigt.

Bürger, lernt Eier zu werfen!

[6] Es handelt sich ja nicht um ein Programm, das einmal entwickelt und dann fortgesetzt benutzt wird, sondern um einen Satz von Werkzeugen, der für jeden Anwendungsfall angepaßt und kontinuierlich weiterentwickelt werden muß.