Von E-Mail-Standorten, mythischen Hackern und Kampfjets

Spiegel offline (von DAUs auch Spiegel „Online“ genannt) und Computer und die Berichterstattung dazu – das passt irgendwie nicht zusammen, Als Quelle der Heiterheit ist es jedoch immer gut. Heute, liebe Kinder, nehmen wir den Standort einer E-Mail durch (ja genau, ihr habt richtig gehört und auch im Internet-Unterricht aufgepasst – brav!) und die chinesische Lockheed Martin F-35 (ja, ein Kampfjet und fast genau so schnell wie eine E-Mail!).

„Spott über Polizei wird Bankräuber zum Verhängnis“, heisst es heute bei SpOff. „Nun schrieb der 19-Jährige in Hamburg eine Mail an Zeitungen und Polizei und machte sich über die Fahnder lustig – wohl ohne zu wissen, dass der Standort jedes Computers ermittelt werden kann. Vier Stunden später nahmen ihn Beamte auf der Reeperbahn in einem Internetcafé fest…“

Wissen wir eigentlich, was gemeint ist? Nicht wirklich. Also lesen wir gemeinsam: „E-Mail-Header lesen und verstehen, dort

das Kapitel „III. E-Mail-Headerzeilen im einzelnen“, genauer: das Unterkapitel „b) „Received:“-Headerzeilen im einzelnen“.

*Received: from mx3.gmx.example (qmailr@mx3.gmx.example [195.63.104.129]) Hier steht jetzt, von welchem Mailserver die E-Mail empfangen wurde. Das Format dieser Zeile ist leider nicht ganz einheitlich. Immer gilt: die Nummer in (eckigen) Klammern ist die unverwechselbare IP-Nummer des einliefernden Rechners – hier „195.63.104.129“. Außerdem ist angegeben, wie dieser sich vorgestellt hat (die Angabe aus dem HELO) – hier „qmailr@mx3.gmx.example“. Das hat unser Mailserver brav überprüft und festgestellt, daß die IP-Nummer tatsächlich zu „mx3.gmx.example“ gehört. (…) Wenn HELO und Realität übereinstimmen, wird der HELO-Parameter manchmal gar nicht angegeben. Dann findet sich nur die IP-Nummer und der (als richtig festgestellte) Name des einliefernden Servers. Andererseits geben manche MTA nur den (möglicherweise gefälschten) HELO-Parameter und die (echte) IP-Nummer an, ohne den zugehörigen Namen nachzuschauen. Dann ist der angegebene Name gerade *nicht* wahr. Auch ist es möglich, daß die Reihenfolge der Angaben genau umgekehrt ist (zuerst HELO, dann tatsächliche Angabe). Schließlich – und am schlimmsten :-(– gibt es ältere MTAs, die noch an das Gute im Menschen glauben und außer dem (beliebig fälschbaren) HELO überhaupt nichts festhalten.*

Alles klar? Puls und Atmung noch normal? Noch mal zum Mitschreiben: Die IP-Adresse ist *nicht* der *Standort* eines Computers, obwohl diejenigen, die an das Märchen der „Online-Durchsuchung“ glauben, das anders sehen (möchten). Was könnte also passiert sein? Hat der doofe Bankräuber seine Webmail-Adresse (DAU-kompatibel: gmx, yahoo, google mail usw.) benutzt, um eine E-Mail an lka.7011@hamburg.de zu schreiben? („Ihre Nachricht wird nur während der normalen Bürostunden gelesen.“ Bankraub bitte nur während der normalen Bürostunden?) Nein, hat er nicht, dann müsste man die Pointe anders formulieren. Im Header der E-Mail wird also die IP-

Adresse eines SMTP-Server gestanden haben, den man dem Internet-Café zuordnen konnte.

Was aber, wenn er ein Laptop und ein offenes WLAN benutzt hätte? Pustekuchen, mal abgesehen von denen, die wissen, wie man eine anonyme E-Mail schreibt. Der Standort eines jeden Computers kann keinesfalls so ermittelt werden. Der Satz ist schlicht grober Blödsinn.

Und jetzt zu etwas ganz Anderem.

Schön ist heute auch die Bildunterschrift einer Spiegel-Offline-Fotostrecke über die „F-35 „Lightning II“: „2009 stahlen Hacker große Mengen an geheimen Daten über das Flugzeug. In den USA wurde China verdächtigt.“ Immer wenn das Wort „Hacker“ in deutschen Medien auftaucht, muss man zwei Mal hinschauen und fragen: Ist das wirklich wahr? Oder wieder nur ein Hoax, ein modernes Märchen oder bewusste Volksverarschung?

Jetzt wird’s lustig – wo haben die das wieder abgeschrieben, ohne zu recherchieren? Wikipedia: „Im April 2009 kam es gemäß einem Bericht des Wall Street Journal zu einem Hackerangriff auf Daten des F-35 Projekts. Dabei wurden größere Mengen Daten aus Rechnern des US-Verteidigungsministeriums gestohlen. Laut Pentagon wurden dabei jedoch keine weitreichend sensiblen Daten kopiert.“

Die Suche nach dem ursprünglichen Tagesschau-Link führt zu Websites, die Verschwörungstheorien verbreiten, die pöhsen Chinesen stünden hinter allem und jedem Byte, das auf eine krumme Bahn gerät – also ungefähr das Niveau der antichinesischen Agitprop, die hierzulande ungefiltert in den Medien breit getreten wird.

In einem ForumGermanicum wird man fündig – dort steht noch die Tagesschau-Meldung von damals:

Unbekannte Computer-Hacker haben einem US-Zeitungsbericht zufolge das teuerste Waffenprojekt in der Geschichte des Pentagon geknackt. Die Täter hätten große Datenmengen aus den Rechnern des US-Verteidigungsministeriums kopiert, darunter auch Detailpläne des neuen Kampfflugzeugs F-35 Lightning II, berichtete das ‚Wall Street Journal unter Berufung auf Regierungskreise. (…) Im Fall des Kampfjets steht der Zeitung zufolge noch nicht fest, wie groß der sicherheitstechnische und finanzielle Schaden ist. Eingedrungen seien die Cyberspione über Schwachstellen in den Netzwerken von zwei oder drei an dem Projekt beteiligten Unternehmen. Zwar hätten die Internetspione mehrere Terabyte an Daten über Design und Elektronik des Kampfflugzeugs abgegriffen. Das geheimste Material sei allerdings sicher geblieben. Es ist demnach auf Computern gespeichert, die nicht mit dem Internet verbunden sind. (…) Pentagon-Sprecher Bryan Whitman kommentierte den Bericht mit dem Hinweis, dass nach seinem Wissen keine sensiblen Daten geknackt worden seien.“

Unter Berufung auf Regierungskreise. Offenbar. Internetspione. Ein seriöses Medium hätte die Quelle verlinkt. „Computer Spies Breach Fighter-Jet Project“, titelte das Wall Street Journal (also *nicht* „einem US-Zeitungsbericht zufolge“ – die Tageschau verschweigt sogar die Quelle und schämt sich noch nicht mal dafür.).

Die Datendiebe sind also in ein schlecht gesichertes Firmennetzwerk eingedrungen, das mit dem des Pentagon

verbunden war. „Former U.S. officials say the attacks appear to have originated in China. However it can be extremely difficult to determine the true origin because it is easy to mask identities online. A Pentagon report issued last month said that the Chinese military has made ’steady progress‘ in developing online-warfare techniques. China hopes its computer skills can help it compensate for an underdeveloped military, the report said.“

Es geht also nur darum, die eigene Schlamperei, das Netzwerk betreffend, als chinesischen „Hacker“-Angriff auszugeben. Nichts Genaues weiß man ohnehin nicht, weil die Journalisten von „ehemaligen“ Angestellten des US-Verteidiungsministeriums gebrieft wurden. Da die Chinesen immer besser und immer böser würden, brauchten die Militärs jetzt mehr Geld – das soll dem Leser suggeriert werden.

Ich glaube wieder mal kein Wort von dem, was in der Zeitung steht, noch nicht mal den Bildunterschriften bei Spiegel offline.