

Trojaner-Sensor

Einen lustigen Hoax bzw. eine Falschmeldung verbreitet [Spiegel Online](#): Aus einem „internen Bericht des Landesverfassungsschutzes“ Baden-Württemberg gehe hervor, dass dort ein „Trojaner-Sensor“ installiert werden soll. „Die Software soll Attacken fremdgesteuerter Spitzelprogramme auf den Behördenrechnern entdecken und abwehren.“

An dem kleinen Text des größten Offline-Nachrichtenmagazins Deutschland ist außer dem Datum, wenn man es genau nimmt, alles falsch bzw. grober Unfug. Die Schlapphüte nutzen also Windows (Trojaner for Apple-Computer oder Linux? Das möchte ich sehen...). Und weil die Anwender keine Ahnung haben, muss noch gesondert Software eingekauft werden, damit man das Geld so richtig zum Schornstein hinauspuften kann.

Aber das ist nicht alles. „Die deutschen Verwaltungen kämpfen bereits seit Jahren gegen elektronische Spionageangriffe, häufig aus Fernost.“ Jetzt verhalten wir uns so, wie sich ein Journalist verhalten würde. Ist diese Meldung wahr: Gibt es mehrere unabhängige Quellen? Ich darf auf zwei Artikel hinweisen., [spiggel.de](#) vom 26.08.2007: „Die China-Hacker kommen nicht“ sowie [spiggel.de](#) vom 04.09.2007: „Chinesen greifen das Pentagon an!“. [Spiegel Online](#) hatte am 26.08.2007 gemeldet: „Der SPIEGEL berichtet in seiner neuen Ausgabe, dass zahlreiche Computer der Bundesregierung mit Spionageprogrammen aus China infiziert sind. Eine Überprüfung, die der Verfassungsschutz und das Bundesamt für Sicherheit in der Informationstechnik vorgenommen haben, kam zu diesem Ergebnis.“ Ich sollte es einfach hier noch einmal posten, weil es so schön ist:

„Jeder, der sich auch nur annähernd mit Computern auskennt, sollte jetzt eigentlich in brüllendes Gelächter ausbrechen. So einen Bären will man uns aufbinden? „Er tarnte sich als Word-Datei oder als Powerpoint-Vortrag“? Wofür soll denn das

Bundesamt für Sicherheit in der Informationstechnik ([BSI](#)) gut sein? Man öffnet auf Windows-Rechnern E-Mails aus Südkorea oder China, mit unbekanntem (?) Absender und – man höre und staune – mit Word-Attachments? Sind die denn total bekloppt? Und so etwas lässt die [EVD-Abteilung](#) unnötig geschehen? Und was soll eine „Umleitung“ sein – können die jetzt sogar IP-Adressen [zuordnen](#)? Wer hätte das gedacht!

Das schreibt das [BSI](#) über G 5.43 Makro-Viren: „Mit dem Austausch von Dateien (z. B. per Datenträger oder E-Mail) besteht die Gefahr, dass neben der eigentlichen Datei (Textdatei, Tabelle etc.) weitere, mit dem Dokument verbundene Makros bzw. eingebettete Editorkommandos übersandt werden. Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.“

Klicken, klicken, klicken, und nicht an die Sicherheit denken? Oder gar Powerpoint? Ceterum censeo: Ich glaube keine Wort. Der *Spiegel* verletzt zudem alle Grundsätze des journalistischen Handwerks, indem er keine, in Worten: keine zwei oder drei unabhängigen Quellen befragt hat, sondern sich ausschließlich auf die Propaganda der Dauerskandalbehörde Verfassungsschutz verlässt. Der baden-württembergische VS-Chef [Johannes Schmalzl](#) darf sich dafür in einem Interview



weitschweifig verbreiten.

Bei [Heise](#)

steht die Meldung auch. Quelle: „der Verfassungsschutz in einem vertraulichen Bericht.“ Weitere Risiko-Faktoren sieht der Verfassungsschutz in der Zunahme der Internet-Telefonie und der Beschäftigung von Praktikanten.“ Bruhaha.

Diese Räuberpistole wurde schon im Februar diesen Jahres in die Welt gesetzt – auch von [Heise](#): „Verfassungsschutz: Spionage aus dem Reich der Mitte bedroht deutschen Mittelstand“. „Dies berichtet die [Financial Times Deutschland](#) (FTD) in ihrer heutigen Ausgabe. „In letzter Zeit haben wir verstärkt chinesische Hackerangriffe festgestellt“, zitiert das Blatt den Vizepräsidenten des Bundesamts für Verfassungsschutz, Hans Elmar Remberg. „Hacker in China sind sehr gut ausgebildet. Sie verfügen über gute mathematische und kryptografische Kenntnisse.“

Sehr hübsch ist [radio-utopie.de](#) zum Thema: Mir scheint, dass der *Spiegel* schlicht auf eine [PR-Offensive](#) der [Result-Group](#) hereingefallen ist:

„Der Vizepräsident des Bundesamts für Verfassungsschutz, Hans Elmar Remberg, bestätigt, dass es einen Anstieg von Wirtschaftsspionage vor allem aus China und Russland gibt. Bereits vor 20 Jahren stellte China mit dem Programm 863 (Ji Hua) die Weichen um die internationale Wettbewerbsfähigkeit in Forschung und Entwicklung von Hochtechnologie zu fördern. Teil des Programms ist die Verpflichtung chinesischer Studenten, die ins Ausland gelassen werden, sich nach ihrer Rückkehr bei der Partei zu revanchieren. Die aktuelle Studie der Result Group zum Thema Informationsabfluss belegt, dass dieses Programm noch heute aktuell ist und in der jüngeren Vergangenheit mehrfach chinesische Studenten, Diplomanden und Praktikanten im Verdacht standen, deutsches Know-how auszuspionieren. Nach Erkenntnissen des Verfassungsschutzes hat sich China zudem auf den Einsatz von Hackern spezialisiert.“

Man braucht nur auf der Website der Result Group GmbH

nachzusehen [Die Links funktionieren nicht mehr, die Sätze wurden gelöscht – warum wohl?): „Unser Erfolg basiert auf einem Netzwerk hoch qualifizierter Spezialisten: Ehemalige Kriminalisten und Sicherheitsbeamte mit weitreichendem Erfahrungspotenzial aus den Spezialeinheiten des Bundes (GSG 9, KSK) und der Länder Spezialeinsatzkommandos (SEK), Mobile Einsatzkommandos (MEK), von BKA, LKA, sowie Verfassungsschutz und BND .“ Auch bei den Kooperationspartnern ist man nicht mehr überrascht – u.a. der [Verband](#) für Sicherheit in der Wirtschaft Baden Württemberg.

Die Result Group schreibt in einer Pressemitteilung vom 04.07 über Afghanistan (!): „Wirksamer Schutz gegen Entführungen im In- und Ausland bietet nur ein professionelles Risiko- und Krisenmanagement. (...) Wirksamer Schutz gegen Entführungen im In- und Ausland bietet nur ein professionelles Risiko- und Krisenmanagement. (...) Besonders kleine- und mittelgroße Firmen sind auf diese Art der Risiken nicht vorbereitet. Das Know-how zum Schutz von Personal und Einrichtungen im gefährdeten Ausland ist meist nicht vorhanden. Diese Lücken schließen dann Beratungsunternehmen wie die Result Group, die seit Jahren erfolgreich nationale und internationale Unternehmen berät. „Man beachte auch einen online [*nicxht mehr*] verfügbaren Vortrag der Result Group (28.02.2007): „Vortrag beim Verband



der bayerischen Wirtschaft – Informationsschutz auf Auslandsreisen (Schwerpunkt China)“.

In einer [Studie der Result Group](#) („Wirtschaftskriminalität durch Informationsabflüsse“) finden sich die vorformulierten Zitate, die die Verfassungsschützer von sich geben, fast wortwörtlich wieder: „Ein ebenfalls unterschätztes Risiko stellen Diplomanden, Praktikanten und Leiharbeiter dar. Der Chef eines mittelständischen Maschinenbau- Unternehmens berichtet: ‚Mir war gar nicht bewußt, dass aus der Beschäftigung des Praktikanten eine Gefahr für mein Unternehmen entstehen könnte.‘ Jetzt wissen wir auch, warum der Verfassungsschutz Praktikanten als Sicherheitsrisikio einstuft.“

Noch Fragen? Die Schleichwerbung eines Unternehmens als Titelstory des *Spiegel* – das hat was.“

Ja, das hat soviel, dass man den gleichen Quatsch zwei Jahre später wieder in die Welt setzt. Merkt eh keiner.