Honeytrap | Unsichere Software

Der Vorstand der German Privacy Foundation bekam kürzlich interessante Post, die ich hier auszugsweise wiedergebe:

“ (…) Am (…) richtete ich auf Ihrer Seite https://privacybox.de/ einen Account in der *PrivacyBox* ein. Unter einem Pseudonym wollte ich auch für Menschen anonym erreichbar sein, welche die in Deutschland m. E. exzessiv ausufernde Staatsschnüffelei nicht für richtig halten.

Bei einem Testlauf startete ich die personalisierte Seite (https://privacybox.de/persoehnlich.msg) aus einem älteren Microsoft Outlook Express Adressbuch (*.wab) heraus, woraufhin der Browser (Firefox 3.0) auf (http://www.theedge.com/) umgeleitet wurde, wo der Fragebogen offensichtlich dem verblüfften User auf die ganz dumme Art Kontaktdaten herauslocken soll. Diesen Server habe ich in Texas, USA, lokalisiert (…). Das Verhalten ist reproduzierbar und geschieht nur bei dieser Webseite, andere werden anstandslos angesteuert. Auch der POP3-Abruf per E-Mail-Programm funktioniert.

Wurde bzw. wird Ihr Dienst, Ihr Server bzw. Ihr Hoster oder auch „nur“ Ihre Seite u. U. von US-Sicherheits-Diensten oder Diensten i. V. m. diesen im Zuge der weltweiten „Terroristenfahndung“ gehackt und missbraucht? Oder ist die Umleitung auf die offensichtlich in den USA gehostete Seite (siehe Anhang!) http://www.theedge.com/ von PrivacyBox und/oder Ihrem Hoster so gewollt?

(…) Die zweite Möglichkeit, dass die gesamte „PrivacyBox“ eine Art von „Honeytrap“ der international zusammenarbeitenden Sicherheitsbehörden ist, in welcher quasi wie in einer „Sandbox“ im Sandkasten – unter Aufsicht der „Erwachsenen“ –

die Unmündigen ihre dummen Geheimnisse austauschen können, mag ich nicht nur nicht ausschließen, sondern das liegt nach meinen Erfahrungen mit ihren Methoden und dieser Seite direkt nahe. (…)“

Ein Vorstandsmitglied hat geantwortet:

“ (…) danke für den Hinweis. (…) Ich habe das Phänomen gerade selbst getestet und komme mit Outlook Express zum selben Ergebnis. Das liegt aber nicht an der PrivacyBox, sondern es ist ein Fehler in Outlook Express, das die URL immer mit einem http:// voran an Firefox übergibt. Sie können die Sache direkt selbst mit beliebigen https-URLs in Firefox testen:

http://https://privacybox.de -> landet bei theedge.com
http://https://www.postbank.de -> ebenfalls

(…) Ich kann versichern, daß die Privacy Foundation die beobachtete Umleitung nicht beabsichtigt hat. Die Box ist kein Honeypot und späht keine Daten im Interesse irgendwelcher Dienste aus. Wir empfehlen Ihnen, veraltete und unsichere Software wie Outlook Express zu meiden.“