netzwoche

01.02.2012 08:38 | Update *01.02.2012 09:29* (Janine Aegerter)

Verschlüsselte Bankendaten

"Selbst ein Supercomputer der US-Behörden könnte diesen Code nicht knacken"

Rolf Haenni arbeitet im "Research Institute for Security in the Information Society" der Berner Fachhochschule in Biel.

Schweizer Banken haben tausende Seiten mit Mails und Bankdaten an die US-Steuerbehörden geliefert. Verschlüsselt, wie vom Bundesrat beteuert wird. Ist das fahrlässig oder ein taktischer Schachzug im Steuerstreit? Die Netzwoche ha bei einem Sicherheitsexperten nachgefragt.

Schweizer Banken haben tausende Seiten mit Mails und anderen Bankdaten an die US-Steuerbehörden geliefert oder planen, dies zu tun. Das hat Schweizer Radio DRS gestern berichtet. Dies würde Daten zum US-Geschäft der Banken betreffen, also beispielsweise Mails, aber keine Kundendaten, wie EFD-Sprecher Roland Meier von Radio DRS zitiert wird. Ausserdem seien die Daten verschlüsselt. Den Codierungsschlüssel sollen die USA erhalten, sobald im Steuerstreit um amerikanischer Steuerhinterzieher eine Lösung gefunden sei. Ist das fahrlässig oder ein taktischer Schachzug im Steuerstreit? Die Netzwoche hat bei einem Sicherheitsexperten nachgefragt.

Herr Haenni, wie gross schätzen Sie die Gefahr ein, dass die US-Behörden die von den Schweizer Banken gelieferte Daten ohne Schweizer Hilfe entschlüsseln können?

Rolf Haenni: Diese Frage lässt sich nicht pauschal beantworten, da wir nicht wissen, welches Verschlüsselungsverfahren angewandt wurde. Wenn wir aber davon ausgehen, dass das gängige Verschlüsselungsverfahren AES angewandt wurde, sehe ich keine realistische Chance, dass die US-Behörden die Daten schon im Voraus entschlüsseln könnten.

Wofür steht AES genau?

AES steht für Advanced Encryption Standard und ist ein symmetrisches Verschlüsselungsverfahren, sprich, für die Verschlüsselung wird der gleiche Schlüssel benutzt wie für die Entschlüsselung. Es gibt verschiedene Verschlüsselungsstärken, AES-128, AES-192 und AES-256. Die Zahlen stehen dabei für die Länge des Schlüssels. J länger dieser ist, desto stärker die Verschlüsselung.

Wie könnte man AES knacken?

Es gibt keine erfolgreichen AES-Attacken, die bekannt sind. Im Prinzip hat man nur die Möglichkeit, alle Schlüssel durchzuprobieren, das wäre im Prinzip die naheliegendste Methode, AES zu knacken. Nur muss man sich bewusst sein, dass selbst bei der schwächsten Verschlüsselung, sprich AES-128, zirka 10 hoch 40 Möglichkeiten an Schlüsseln zur Verfügung stehen. Bei AES-256 erhöht sich diese Zahl auf etwa 10 hoch 80 mögliche Schlüssel. Dies Zahl entspricht in etwa der Menge an Atomen, die in unserem Weltall herumschwirren. Selbst ein Supercomputer der US-Behörden könnte diesen Code also nicht innert einer nützlichen Frist knacken.

Könnten Sie dies noch etwas konkreter erklären?

Wenn man mit einem sehr schnellen Computer 1 Milliarde (10 hoch 9) Schlüssel pro Sekunde durchprobiert, dann schafft man pro Jahr ungefähr 10 hoch 17 Schlüssel, d.h. bei AES-128 würde es immer noch etwa 10 hoch 23 Jahre dauern, beziehungsweise bei AES-256 sogar 10 hoch 63 Jahre, also viel, viel länger als das Alter des Universums. Daran ändert sich auch nichts wenn man 1 Milliarde solcher Computer gleichzeitig benutzt, denn das reduziert die Anzahl Rechenjahre immer noch auf 10 hoch 14 beziehungsweise 10 hoch 54. Folglich ist dieses Unterfangen selbst mit allen existierenden Computern absolut aussichtslos.

Dann sehen Sie im Vorgehen des Bundesrates keine Probleme?

Ich denke, es ist sicher ein taktische Entscheidung. Ich kann diese Frage aber nicht beantworten, da wir ja wie gesagt nicht wissen, welcher Verschlüsselungsstandard verwendet wurde. Unter der Annahme, dass tatsächlich AES eingesetzt wurde, sehe ich aus einer rein technischen Sicht aber kein Problem bei der Entscheidung des Bundesrates, nein.

Anmerkung der Redaktion: Rolf Haenni ist Dozent der Berner Fachhochschule (BFH) in Biel und arbeitet im "Research Institute for Security in the Information Society" der BFH Biel.

politics, software, e-security, banking

Kommentar

Ihr Kommentar (max. 400 Zeichen)

Code-nicht-knacken.aspx?pa=1