

Nach den neuesten Snowden Enthüllungen: Keine Backdoor in der deutschen Verschlüsselungssoftware Boxcryptor

Boxcryptor – die Verschlüsselungslösung für Dropbox und viele weitere Cloudspeicheranbieter reagiert auf die neuen Enthüllungen von Edward Snowden. Dieser offenbarte, dass einige Hersteller von Verschlüsselungslösungen Hintertüren (sog. Backdoors) für die NSA in ihrer Software implementiert haben. Die Geschäftsführung der Secomba GmbH betont heute, dass es in der deutschen Verschlüsselungssoftware keine solchen Backdoors gibt.

Augsburg, 06.09.2013: Der Guardian und die New York Times haben heute auf Grundlage von geheimen Dokumenten die durch Edward Snowden an die Öffentlichkeit gelangt sind beunruhigende Neuigkeiten veröffentlicht. Snowden zufolge ist der amerikanische Geheimdienst (NSA) in der Lage vermeintlich sichere Kommunikation die über HTTPS, SSL und Voice-Over-IP erfolgt zu entschlüsseln. Des Weiteren wurde enthüllt, dass einige – nicht konkret benannte – Unternehmen Backdoors in ihrer Software eingebaut haben, um der NSA die schnelle und einfache Entschlüsselung der Nutzerdaten zu ermöglichen.

Diese Neuigkeiten sind nicht nur für Anwender von Verschlüsselungslösungen beunruhigend, sondern für alle Internetnutzer weltweit. Dabei ist für die Entwicklung von Verschlüsselungssoftware nicht nur ein hohes technisches Wissen erforderlich, sondern der Hersteller benötigt auch ein hohes Maß an Vertrauen von den eigenen Nutzern. Dieses Vertrauen wird nun stark erschüttert. „Aus diesem Grund haben wir uns entschieden, auf diese Enthüllungen zu reagieren und unsere Nutzer wissen zu lassen, dass ihre Daten bei der Nutzung von Boxcryptor geschützt sind.“, so Robert Freudenreich, Gründer und Geschäftsführer der Secomba GmbH.

Laut Freudenreich verwendet Boxcryptor zur Kommunikation mit den eigenen Servern HTTPS. Da Boxcryptor allerdings ein Zero-Knowledge Anbieter ist, wird sämtliche sensible Information die an den Server geschickt wird bereits auf dem Gerät des Nutzers vor der eigentlichen Übertragung mit dem Passwort des Nutzers verschlüsselt (z.B. private RSA Schlüssel) oder ist anderweitig nicht abrufbar (wie z.B. der Passwort Hash) und somit geschützt. Des Weiteren verwendet Boxcryptor als Public-Key Verfahren RSA mit 4096-Bit Schlüsseln anstelle einer Elliptische-Kurven-Kryptographie, die durch die neuen Enthüllungen unter Verdacht geraten ist. Selbst wenn die NSA nun die mit HTTPS geschützte Kommunikation zwischen dem Nutzer und dem Boxcryptor Server abfangen können sollte, kann der Geheimdienst lediglich immer noch verschlüsselte Daten sehen und hieraus keine Informationen ableiten.

Freudenreich betont: “Wir sind ein deutsches Unternehmen mit Sitz in Augsburg und können weder durch die US Regierung noch durch andere Organisationen dazu gezwungen werden, eine Backdoor oder ähnliches in unsere Software einzubauen. Als Gründer und Geschäftsführer der Secomba GmbH versichern wir, dass Boxcryptor keine solche Vorkehrung hat, hatte oder jemals haben wird, welche das Recht unserer Nutzer auf Datenschutz untergräbt.”

Secomba GmbH

Andrea Pfundmeier
Werner-von-Siemens-Str. 6
86159 Augsburg

www.boxcryptor.com

tel: +49 (0821) 907 861 51
fax: +49 (0821) 907 861 59
mail: ap@secomba.com

Die Secomba GmbH – gegründet 2011 mit Sitz in Augsburg - wurde in der Startphase vom Bundesministerium für Wirtschaft und Technologie im Rahmen des EXIST-Gründerstipendiums unterstützt. 2012 wurde BoxCryptor unter anderem von der Telekom im Rahmen des Telekom Innovationspreis mit dem 2. Platz sowie dem Publikumspreis ausgezeichnet.