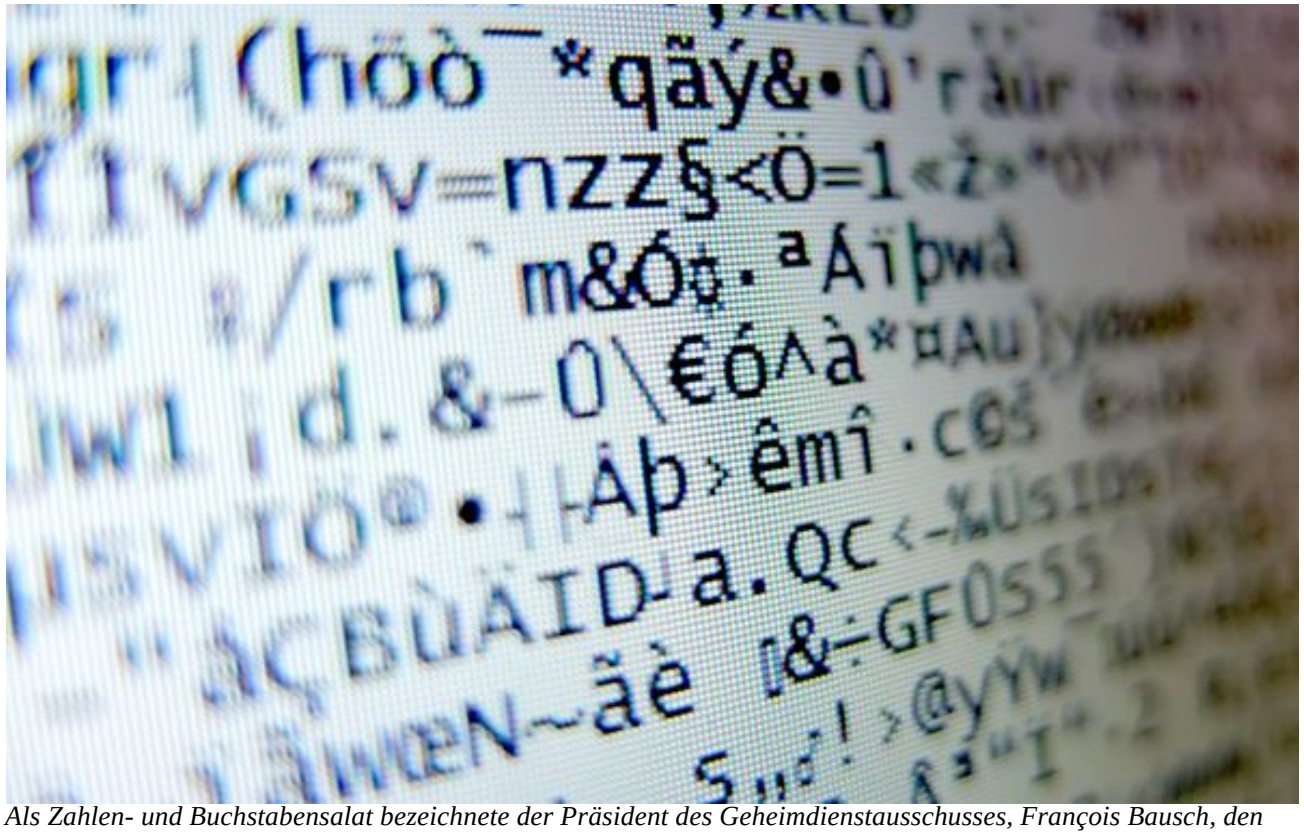
Luxemburger Wort

Bommeleeër: Der Schlüssel zur CD



Als Zahlen- und Buchstabensalat bezeichnete der Präsident des Geheimdienstausschusses, François Bausch, den Inhalt der Daten-CD.
Foto: Steve Remesch
(#)

Veröffentlicht am Freitag, 30. November 2012 um 13:23

(str) - In Geheimdienstkreisen gibt es eine CD, von der es heißt, darauf sei eine illegale Aufnahme von einem Gespräch zwischen Jean-Claude Juncker und Großherzog Henri über die Bommeleeër-Affäre. Die CD ist verschlüsselt und bislang ist es offenbar nicht gelungen, diese zu entschlüsseln.

Obwohl, einmal schon! Wie **„d'Lëtzebuerger Land" (http://www.land.lu/)** am Freitag berichtet sei es einem gewissen M. gelungen, den Datenträger auszulesen. Der Name ist ein Initial und hat nichts mit einer gleichnamigen James Bond-Figur gemein.

Wie aus dem am **Freitag veröffentlichten Protokoll der Aufnahme des Juncker-Mille-Gesprächs (http://www.wort.lu/de/view/im-geheimdienst-ihrer-majestaet-50b86275e4b0bb8c16c8ff6c)** hervorgeht, habe M. in der Vergangenheit mit dem Luxemburger Geheimdienst zusammen garbeitet. Ihm, als versierter Techniker, sei die CD vom Großherzoglichen Hof zugespielt worden, um diese zu dechiffrieren. M. soll seinen Auftraggebern gesagt haben, das sei ihm nicht gelungen. Eine Lüge! In Wirklichkeit sei es ihm sehr wohl gelungen, die CD auszulesen. Zudem habe er eine Kopie an den Geheimdienst weitergeleitet. Dem sei die Dekryptierung aber widerum nicht gelungen. Ob der Dienst aber noch einmal auf die Hilfe von M. zurückgegriffen hat, bleibt unklar.

Kryptovox und Crypto-Box

Im „Land“ werden am Freitag zwei verschiedene Namen für die verwendeten Verschlüsselungsprozeduren genannt: Kryptovox und Crypto-Box. Bei Kryptovox handelt es sich um einen Algorithmus, der für die Verschlüsselung von Telefongesprächen verwendet wird und der bereits zu Beginn der 1990er Jahre ausgearbeitet wurde.

Crypto-Box ist ein Produkt des deutsch-amerikanischen Herstellers **Marx Software Security (http://www.cryptotech.com/products_cryptobox2.php)** . „Dabei handelt es sich um eine sogenannte Zwei-Faktoren-Verschlüsselung“, erklärt Jan Guth, der Präsident des **Chaos Computer Clubs Luxemburg (C3L) (http://c3l.lu/)** gegenüber wort.lu. „Dabei wird eine Datei gleichermaßen von einer Software als auch von einer Hardware, in diesem Fall einem sehr leistungsfähigen USB-Stick, verschlüsselt.“

Zugang über das Hintertürchen?

Das Verfahren entspricht der „EAL 4+“-Norm, eine Verschlüsselung auf der vierten von sieben Ebenen und gilt als sehr sicher. Sam Grüneisen, ebenfalls vom C3L, betont allerdings, dass die Zwei-Faktoren-Verschlüsselung auch ihre Tücken habe. „Dieses Verfahren könnte eine Entschlüsselung vereinfachen, denn die Kombination von Software und Hardware birgt oft Schwachstellen bei der Software“, so der Hacker. „Zudem bauen Hersteller oft Backdoors ein oder erlauben den Zugriff mit einem Master-Passwort.“

„Die Chancen, verschlüsselte Daten zu dechiffrieren, hängen immer von der Länge der Passwörter ab“, erklärt Jan Guth. „Geheimdienste verwenden standardmäßig eine 128-bit AES-Codierung. Die ist rein mathematisch nicht einfach zu knacken. Gelingt es einem allerdings per Zufallsgenerator auf das richtige Passwort zu kommen, dann kann es aber auch sehr schnell gehen. Bei einem 16-stelligen Passwort, kann das aber auch Jahre dauern.“

Keine Audiodatei?

Verwundert zeigen sich die beiden Hacker allerdings über die Aussage von Geheimdienstverantwortlichen gegenüber der Kontrollkommission, dass es sich mit großer Wahrscheinlichkeit bei den verschlüsselten Daten nicht um ein Ton-Dokument handele. „Beim mathematischen Algorithmus einer Datei kann man im Prinzip aus dem Header erfahren, um welche Datei es sich handelt“, betont Jan Guth. „Bei einer verschlüsselten Datei kann man ein bestimmtes Format aber nicht von vorne herein ausschließen.“ Außerdem entspreche die Dateigröße in etwa jener einer einstündigen Tonaufnahme.

Nicht ausschließen wollen die Hacker zudem, dass es sich bei der CD um ein Ablenkungsmanöver handeln könnte. „Ein Fake ist mit Linux sehr einfach zu erstellen“, unterstreicht Sam Grüneisen. "Es reicht einen Zufallscode zu generieren und den auf eine bestimmte Datengröße auszudehnen.“

Der **Chaos Computer Club Luxemburg (http://c3l.lu/)** ist eine Gruppe von Hackern, bestehend aus Informatikern, Mathematikern, Physiker und auch Erziehern, die sich Informationssicherheit und Datenschutz auf die Fahne geschrieben haben. Die Gruppe hat sich zum Ziel gesetzt Schwachstellen aufzudecken und Nutzer über Sicherheit und Gefahren aufzuklären.

„Falls der Geheimdienst auf unsere Kompetenzen zurückgreifen will, stehen wir natürlich mit Rat und Tat bereit“, meint Jan Guth abschließend.