Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

[redacted]

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 9582-0
FAX +49 228 99 9582-5400

referat-b21@bsi.bund.de
https://www.bsi.bund.de

Betreff: Anfrage nach dem Informationsfreiheitsgesetz
hier: Bescheid des BSI

Bezug: Ihre Anfrage vom 17.07.2016
Aktenzeichen: B21- 010 [redacted]
Datum: 17.08.2016

Anlage: - Bericht des BSI an BMI vom 29.05.2015
- BT-Drucksache 18/5144 vom 11.06.2015

[redacted]

auf Ihre o.g. Anfrage ergeht folgender

Bescheid

1. Ihrem Antrag wird stattgegeben.
2. Es werden keine Gebühren erhoben.

Begründung

1.

Mit Ihrer Anfrage vom 17.07.2016 baten Sie um Übersendung sämtlicher internen Bewertungen oder Stellungnahmen gegenüber Bundesbehörden/-ministerien seit 1990, die sich mit der Bewertung oder Einschätzung der Eckpunkte deutscher Kryptopolitik befassen.

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen hierzu zwei Dokumente vor. Das erste Dokument „Erfahrungsbericht Kryptoeckpunkte" ist ein Erfahrungsbericht verschiedener Behörden zu den Eckpunkten deutscher Kryptopolitik aus dem Jahr 2001. Folgende Bewertung wurde durch das BSI beigesteuert:

„Seitens des BSI wird darauf hingewiesen, dass bei starken Verschlüsselungsverfahren nach heutigen Erkenntnissen eine zeitnahe Entschlüsselung nur dann erfolgen kann, wenn Verfahren und Schlüssel bekannt sind. Mit vertretbarem Aufwand können heute 40-Bit-Verschlüsselungen „problemlos" gelöst werden, bei 50 Bit würde die Bearbeitungszeit bereits um das tausendfache ansteigen, bei 60 Bit würde die Lösung 1 Million mal länger dauern. Wäre man also so fantastisch schnell, dass man zur Lösung von 40 Bit nur eine Minute benötigt, so würden 60 Bit schon fast 2 Jahre in Anspruch nehmen.
Ein gutes 128-Bit-Verfahren (kommerziell erhältlich), ist also zurzeit, unabhängig vom Aufwand der zur Dechiffrierung betrieben wird, zeitnah nicht zu lösen.
Der Einsatz von Quantencomputern, so sie denn Wirklichkeit werden, könnte die Situation evtl. Ändern.
Es ist demnach sehr fraglich, ob die Einrichtung von Stellen, die eine zeitnahe Entschlüsselung bieten sollen, den gewünschten Erfolg bringen können.
Nach wie vor werden sich die Möglichkeiten darauf beschränken, die verwendeten Kryptoprodukte auf evtl. Schwachstellen oder Implementierungsfehler zu untersuchen. Diese Methode ist sehr aufwendig und langwierig. Insbesondere dann, wenn Eigenentwicklungen benutzt werden, bei denen lediglich das verschlüsselte Datenmaterial und nicht das Verfahren an sich zur Verfügung steht, sind die Erfolgsaussichten eher gering."

Da BSI bezüglich der weiteren Beiträge dieses Erfahrungsberichts nicht die verfügungsberechtigte Behörde gem. § 7 Absatz 1 IFG ist, kann Ihnen das Dokument nicht übersandt werden.

Das zweite Dokument ist ein Bericht des BSI vom 29.05.2015 auf einen Erlass des Bundesministerium des Innern (BMI). Anlass für den Erlass des BMI ist eine Kleine Anfrage der Fraktion DIE LINKE (BT Drucksache 18/5013) zu den Anstrengungen von Europol, INTERPOL und der Europäischen Kommission zum Aushebeln von Verschlüsselungstechniken.

BSI wurde um die Beantwortung der Fragen 7, 8, 9 und 10 gebeten (s. Anlage). Relevant für Ihre Anfrage ist die Antwort des BSI zu Frage 10.
Punkt III zu Frage 7 wurde geschwärzt, da gemäß § 3 Nr. 4 IFG ein Anspruch auf Informationszugang nicht besteht, wenn die Information einer durch Rechtsvorschrift oder durch die Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen geregelten Geheimhaltungs- oder Vertraulichkeitspflicht unterliegt. Dieser Ausnahmetatbestand liegt vor, da die von Ihnen begehrte Information als geheimhaltungsbedürftige Tatsachen und Erkenntnisse im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Verschlusssachenanweisung (VSA) als Verschlusssache eingestuft wurde. Die Informationen dürfen damit gemäß § 4 Abs.1 VSA nur Personen zugänglich gemacht werden, die aufgrund ihrer Dienstpflichten von diesen Kenntnis haben müssen.
Zu Ihrer Information habe ich Ihnen die komplette Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE beigefügt (BT-Drucksache 18/5144).

2.
Da es sich bei Ihrer Anfrage um eine einfache Anfrage handelt, werden gem. § 10 Abs. 1 IFG keine Gebühren oder Auslagen erhoben.

Rechtsbehelfsbelehrung
Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe beim Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Widerspruch erhoben werden.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Julia Steig