[redacted]

[redacted]

Datum
2020-03-01

Betr.: Widerspruch Bescheid "Trusted Disk"

Sehr geehrte Frau Steig,

Mit Datum vom 21.02.2020 haben Sie mir einen Bescheid zu meiner Anfrage nach dem Informationsfreiheitsgesetz nach bei Ihnen vorliegenden Analysen zur Software Trusted Disk (Geschäftszeichen BL23 - 010 03 05/2020-004) zukommen lassen.

Ich lege hiermit Widerspruch gegen den Bescheid ein.

Sie lehnen meine Anfrage unter Berufung auf §3 Nr. 4 IFG ab, da es sich um ein als geheim eingestuftes Dokument handelt.

Ich verweise hierbei darauf, dass das Bundesverwaltungsgericht in einem Urteil (Urteil vom 29.10.2009 - BVerwG 7 C 21.08) festgestellt hat: "Der Anspruch auf Zugang zu einer Information ist nicht allein deshalb nach § 3 Nr. 4 IFG ausgeschlossen, weil die Information formal als Verschlusssache eingestuft ist. Vielmehr kommt es darauf an, ob die materiellen Gründe für eine solche Einstufung vorliegen."

Ich sehe in Ihrem Bescheid keine materiellen Gründe für eine solche Einstufung.

Sie verweisen darauf, dass "sich das Produkt im aktiven Betrieb befindet und eine Veröffentlichung der Informationen die Sicherheit des Produktes herabsetzen kann". Diese Begründung legt nahe, dass in den fraglichen Dokumenten Sicherheitsprobleme des fraglichen Produkts beschrieben sind. Falls dies der Fall ist wäre das allerdings maximal eine Begründung, die Herausgabe der Informationen zu verzögern, bis diese Sicherheitsprobleme behoben sind.

Es ist allgemein anerkannt, dass die generelle Geheimhaltung von Sicherheitsproblemen - auch Security by Obscurity genannt - keine sinnvolle Strategie der IT-Sicherheit ist. Ich möchte hierzu auf eine von Ihrer Behörde selbst veröffentlichte Broschüre [1] verweisen:

> "Viele Unternehmen verfolgen bei der Information über Schwachstellen häufig das Prinzip 'Security by Obscurity', d. h. es werden keine oder nur unzureichende Informatio-nen über mitunter gravierende Schwachstellen veröffentlicht.

[redacted]

Jedoch kann gerade diese Denkweise dazu führen, dass Angreifer solche Schwachstellen ausnutzen, wenn sie bereits durch eigene Erkenntnisse oder den Zukauf aus entsprechenden Quellen bekannt sind. In letzter Konsequenz werden somit die Anwender der betroffenen Softwareprodukte geschädigt."

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_019.pdf

Mit freundlichen Grüßen

[redacted]