Joachim Lindenberg

Von: GP IFG <[redacted]@bsi.bund.de>
Gesendet: Monday, 19 July 2021 13:53
An: [redacted]
Cc: GP IFG
Betreff: Bescheid zu Ihrer IFG-Anfrage Verschlüsselung im BSI Grundschutz? [# 224475]
Anlagen: 20210719_Bescheid Lindenberg.pdf

Sehr geehrter Herr Lindenberg,

anbei übersende ich Ihnen meinen Bescheid zu Ihrer Anfrage nach dem Informationsfreiheitsgesetz (IFG) vom 07.07.2021.

Ich möchte Sie darauf hinweisen, dass es sich bei Ihrer Anfrage inhaltlich nicht um eine Anfrage nach dem Informationsfreiheitsgesetz (IFG) handelt, da es sich hierbei um Verständnisfragen handelt und diese sich nicht auf bereits vorhandene Informationen beziehen. Ich habe die zuständigen Kollegen um Beantwortung Ihrer Fragen gebeten und möchte Ihnen die Antwort untenstehend übersenden:

Leider kann der IT-Grundschutz nur sehr eingeschränkt auf Aspekte des Datenschutzes eingehen, da dies nicht der gesetzliche Auftrag des BSI ist. Gleichwohl ist aber klar, dass die Themen Informationssicherheit und Datenschutz immer näher zusammenwachsen, weswegen das Thema Datenschutz in ausgewählten Bereichen des IT-Grundschutzes als Schnittstellenthema dargestellt wird. In diesem Sinne ist auch der IT-Grundschutz-Baustein CON.2 Datenschutz zu verstehen.

Ihrer Anfrage entnehmen wir neben der umfangreichen Schilderung der Ausgangslage im Kern die folgende Frage:

"Im Ergebnis kann eine Organisation nach BSI Grundschutz zertifiziert werden, ohne Verschlüsselung zu verwenden. Und das soll mir oder einem anderen Bürger Vertrauen in eine BSI Zertifizierung geben?"

Das ist so nicht korrekt, bedarf aber weiterer Erläuterungen. Der IT-Grundschutz stellt ein ISMS (Managementsystem für Informationssicherheit) dar und betrachtet das Thema Informationssicherheit ganzheitlich. Folglich können für die Bewertung der Informationssicherheit nicht einzelne Aspekte des Managementsystems bzw. einzelne IT-Grundschutz-Bausteine betrachtet werden, sondern es müssen immer alle relevanten Bausteine/Aspekte betrachtet werden. Konkret bedeutet dies, dass im Baustein CON.1 Kryptokonzept übergreifende Aspekte hinsichtlich der Kryptographie thematisiert werden (die Bausteinschicht CON betrachtet Konzepte und Vorgehensweisen). Spezifische Aspekte zur Kryptographie, die nur für konkrete Zielobjekte relevant sind, werden jedoch in weiteren Bausteinen behandelt. Hier seien nur folgende Anforderungen aus den entsprechenden Bausteinen exemplarisch genannt:

- APP.1.2.A2 Unterstützung sicherer Verschlüsselung der Kommunikation (B) macht Vorgaben an die Transportverschlüsselung beim Einsatz von Webbrowsern
- SYS.3.1.A13 Verschlüsselung von Laptops (S) macht Vorgaben hinsichtlich der Verschlüsselung von Datenträgern in Laptops
- SYS.2.1.A28 Verschlüsselung der Clients (H) macht Vorgaben hinsichtlich der Verschlüsselung von schutzbedürftigen Daten auf Clients
- NET.1.1.A7 Absicherung von schützenswerten Informationen (B) regelt, in welchen Szenarien Netzverbindungen verschlüsselt werden müssen
- SYS.1.8.A23 Einsatz von Verschlüsselung für Speicherlösungen (H) macht Vorgaben hinsichtlich der Verschlüsselung von in Speicherlösungen abgelegten Daten
- SYS.4.5.A10 Datenträgerverschlüsselung (B) macht Vorgaben für Szenarien, in denen Wechseldatenträger verschlüsselt werden müssen

Basis-Anforderungen (B) müssen uneingeschränkt erfüllt werden. Es gilt zu berücksichtigen, dass auch Standard-Anforderungen (SOLLTE-Anforderungen, mit (S) markiert) gemäß BSI-Standard 200-2 grundsätzlich umzusetzen sind: „Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden."

Da der IT-Grundschutz auf einen normalen Schutzbedarf zielt, sind die Anforderungen bei erhöhtem Schutzbedarf (H) exemplarische Vorschläge aus der Praxis, die berücksichtigt werden können, wenn ein entsprechender Schutzbedarf der betroffenen Informationen vorliegt. Bei erhöhtem Schutzbedarf erfordert die IT-Grundschutz-Methodik aber in jedem Fall die Durchführung und Dokumentation einer zusätzlichen Risikoanalyse.

Die im BSI-Standard 200-2 beschriebene Schutzbedarfsfeststellung stellt unter Berücksichtigung der Anforderungen aus dem Datenschutz (2. Schadensszenario: Beeinträchtigung des informationellen Selbstbestimmungsrechts) sicher, dass solche Informationen identifiziert und in der weiteren Folge des Sicherheitsprozesses nach IT-Grundschutz angemessen abgesichert werden.

Dies alles wird im Rahmen einer ISO-27001-Zertifizierung auf Basis von IT-Grundschutz überprüft. Es ist somit praktisch ausgeschlossen, dass eine Institution eine solche Zertifizierung erhält, ohne angemessen Verschlüsselung einzusetzen.

Für fachliche und inhaltliche Rückfragen steht das IT-Grundschutz-Referat gerne unter it-grundschutz@bsi.bund.de zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Referat BL23 - IT-Sicherheit und Recht
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 - 189
53175 Bonn

Telefon: +49 (0)228 99 9582 0
Telefax: +49 (0)228 99 9582 6767
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalsicherBSI

-----Ursprüngliche Nachricht-----
Von: Joachim Lindenberg [#224475] <j.lindenberg.ugd8e5y2tk@fragdenstaat.de>
Gesendet: Mittwoch, 7. Juli 2021 15:19
An: GP IFG <[redacted]@bsi.bund.de>
Betreff: Verschlüsselung im BSI Grundschutz? [#224475]

Antrag nach dem IFG/UIG/VIG

Sehr geehrte Damen und Herren,

bitte senden Sie mir Folgendes zu:

Die DSGVO erwähnt in Artikel 32 (1) Verschlüsselung als geeignetes Mittel zum Schutz personenbezogener Daten. Das ist nicht wirklich neu, schon die Anlage zum alten BDSG §9 erwähnte Verschlüsselung als geeignetes Mittel.

Besonders deutlich ist das neue BDSG im §64 oder z.B. das LDSG SH in §40 jeweils im gleichlautenden Absatz (3) jeweils letzter Satz - beide natürlich nur im Bereich der EU Richtlinie 680/2016 direkt anwendbar. Dort steht "Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden." Daraus leite ich eine Empfehlung des Gesetzgebers ab, Verschlüsselung entsprechend dem Stand der Technik zu verwenden oder darzulegen wie die Nummern 2 bis 5 anders gleichwertig sichergestellt werden können - und beim besten Willen - dieser Nachweis der Gleichwertigkeit wird nach meiner Erfahrung gerne vernachlässigt. Und auch wenn BDSG Teil 3 nur für die Justiz direkt gültig ist - viele Vorschriften dort sind nur Konkretisierungen von Erwartungen auch im Anwendungsbereich der DSGVO.

Leider ist der BSI Grundschutz - und der findet auch im Bereich der EU Richtlinie 680/2016 Anwendung - da sehr unklar. Warum? Weil nicht nur personenbezogene Daten verarbeitet werden können? In der Realität sind die allermeisten Daten die verarbeitet werden möglicherweise irgendwie personenbezogen, und sei es nur über Metadaten oder Protokolle. Insofern muss meiner Meinung nach die Empfehlung sein, lieber zu viel als zu wenig zu verschlüsseln.

Leider geht der Baustein CON.1 auf diese Problematik überhaupt nicht ein. Er zählt - von der Einleitung abgesehen - mehr die Probleme von unprofessionell umgesetzter Verschlüsselung auf, als Organisationen dazu aufzufordern, Verschlüsselung als Standard zu etablieren. So sind viele Anfoderungen in CON.1 ein SOLL statt ein MUSS, und eine Anforderung personenbezogene oder andere vertrauliche Daten zu verschlüsseln fehlt vollständig. Selbst bei Daten mit hohem Schutzbedarf steht nur ein SOLL, kein MUSS.

Im Ergebnis kann eine Organisation nach BSI Grundschutz zertifiziert werden, ohne Verschlüsselung zu verwenden. Und das soll mir oder einem anderen Bürger Vertrauen in eine BSI Zertifizierung geben?

Dies ist ein Antrag auf Zugang zu amtlichen Informationen nach § 1 des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (IFG) sowie § 3 Umweltinformationsgesetz (UIG), soweit Umweltinformationen im Sinne des § 2 Abs. 3 UIG betroffen sind, sowie § 1 des Gesetzes zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (VIG), soweit Informationen im Sinne des § 1 Abs. 1 VIG betroffen sind.

Sollte der Informationszugang Ihres Erachtens gebührenpflichtig sein, möchte ich Sie bitten, mir dies vorab mitzuteilen und detailliert die zu erwartenden Kosten aufzuschlüsseln. Meines Erachtens handelt es sich um eine einfache Auskunft. Gebühren fallen somit nach § 10 IFG bzw. den anderen Vorschriften nicht an. Auslagen dürfen nach BVerwG 7 C 6.15 nicht berechnet werden. Sollten Sie Gebühren veranschlagen wollen, bitte ich gemäß § 2 IFGGebV um Befreiung oder hilfweise Ermäßigung der Gebühren.

Ich verweise auf § 7 Abs. 5 IFG/§ 3 Abs. 3 Satz 2 Nr. 1 UIG/§ 4 Abs. 2 VIG und bitte Sie, mir die erbetenen Informationen so schnell wie möglich, spätestens nach Ablauf eines Monats zugänglich zu machen. Kann diese Frist nicht eingehalten werden, müssen Sie mich darüber innerhalb der Frist informieren.

Ich bitte Sie um eine Antwort per E-Mail gemäß § 1 Abs. 2 IFG. Ich widerspreche ausdrücklich der Weitergabe meiner Daten an behördenexterne Dritte. Sollten Sie meinen Antrag ablehnen wollen, bitte ich um Mitteilung der Dokumententitel und eine ausführliche Begründung.

Ich möchte Sie um eine Empfangsbestätigung bitten und danke Ihnen für Ihre Mühe!

Mit freundlichen Grüßen

Joachim Lindenberg

Anfragenr: 224475
Antwort an: j.lindenberg.ugd8e5y2tk@fragdenstaat.de
Laden Sie große Dateien zu dieser Anfrage hier hoch:
https://fragdenstaat.de/anfrage/224475/upload/392517fec8632d72abbc3cc847fba6226f13ef50/

Postanschrift
Joachim Lindenberg
[redacted]

--
Rechtshinweis: Diese E-Mail wurde über den Webservice fragdenstaat.de versendet. Antworten werden ggf. im Auftrag der Antragstellenden auf dem Internet-Portal veröffentlicht.
Falls Sie Fragen dazu haben oder eine Idee, was für eine Anfrage bei Ihnen im Haus notwendig wäre, besuchen Sie: https://fragdenstaat.de/hilfe/fuer-behoerden/

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Joachim Lindenberg
[redacted]

Nur per E-Mail:
[redacted]

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582-0
Fax +49 228 99 9582-6767

[redacted]@bsi.bund.de

www.bsi.bund.de

DE-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Ihre Anfrage nach dem Informationsfreiheitsgesetz (IFG)

Bezug: Ihre Anfrage vom 07.07.2021
Geschäftszeichen: BL23 – 010 03 05/ 2021-047
Datum: 19.07.2021

Sehr geehrter Herr Lindenberg,

auf Ihre Anfrage nach dem Informationsfreiheitsgesetz (IFG) vom 07.07.2021 ergeht folgender

Bescheid

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

Begründung
1.
In Ihrem oben genannten Antrag nach dem Informationsfreiheitgesetz bitten Sie um Übersendung folgender Informationen:

„Die DSGVO erwähnt in Artikel 32 (1) Verschlüsselung als geeignetes Mittel zum Schutz personenbezogener Daten. Das ist nicht wirklich neu, schon die Anlage zum alten BDSG §9 erwähnte Verschlüsselung als geeignetes Mittel. Besonders deutlich ist das neue BDSG im §64 oder z.B. das LDSG SH in §40 jeweils im gleichlautenden Absatz (3) jeweils letzter Satz - beide natürlich nur im Bereich der EU Richtlinie 680/2016 direkt anwendbar. Dort steht "Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden." Daraus leite ich eine Empfehlung des Gesetzgebers ab, Verschlüsselung entsprechend dem Stand der Technik zu verwenden oder darzulegen wie die Nummern 2 bis 5 anders gleichwertig sichergestellt werden können - und beim besten Willen - dieser Nachweis der Gleichwertigkeit wird nach meiner Erfahrung gerne vernachlässigt. Und auch wenn BDSG Teil 3 nur für die Justiz direkt gültig ist - viele Vorschriften dort sind nur Konkretisierungen von Erwartungen auch im Anwendungsbereich der DSGVO.

Leider ist der BSI Grundschutz - und der findet auch im Bereich der EU Richtlinie 680/2016 Anwendung - da sehr unklar. Warum? Weil nicht nur personenbezogene Daten verarbeitet werden können? In der Realität sind die allermeisten Daten die verarbeitet werden möglicherweise irgendwie personenbezogen, und sei es nur über Metadaten oder Protokolle. Insofern muss meiner Meinung nach die Empfehlung sein, lieber zu viel als zu wenig zu verschlüsseln.

Leider geht der Baustein CON.1 auf diese Problematik überhaupt nicht ein. Er zählt - von der Einleitung abgesehen - mehr die Probleme von unprofessionell umgesetzter Verschlüsselung auf, als Organisationen dazu aufzufordern, Verschlüsselung als Standard zu etablieren. So sind viele Anforderungen in CON.1 ein SOLL statt ein MUSS, und eine Anforderung personenbezogene oder andere vertrauliche Daten zu verschlüsseln fehlt vollständig. Selbst bei Daten mit hohem Schutzbedarf steht nur ein SOLL, kein MUSS.

Im Ergebnis kann eine Organisation nach BSI Grundschutz zertifiziert werden, ohne Verschlüsselung zu verwenden. Und das soll mir oder einem anderen Bürger Vertrauen in eine BSI Zertifizierung geben?"

Die gewünschten Informationen liegen im Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht vor.

2.
Bei Ihrer Anfrage handelt es sich um eine einfache Anfrage im Sinne des § 10 Abs. 1 S. 2 IFG. Es werden keine Gebühren 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]