



POSTANSCHRIFT ITZBund, Postfach 30 16 45, 53 196 Bonn

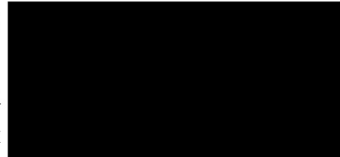


Nur per E-Mail:



HAUSANSCHRIFT Dienstsitz Bonn  
Bernkasteler Str. 8, 53175 Bonn

BEARBEITET VON



TEL

FAX

E-MAIL IFG@ITZBund.de

DATUM 27.09.2022

BETREFF Informationsfreiheitsgesetz des Bundes (IFG);

**Dokumente zum CERT (Computer Emergency Response Team) [#258726]**

BEZUG Ihr Antrag vom 9. September 2022

ANLAGEN keine

GZ 03010302#00002#0097

Sehr geehrte(r)



mit E-Mail vom 9. September 2022 beantragen Sie nach dem Informationsfreiheitsgesetz des Bundes (IFG) Zugang zu folgenden Informationen:

„Dokumente zum CERT (Computer Emergency Response Team) innerhalb des ITZBund's.

Dies beinhaltet:

- ob es ein solches Team intern beim ITZBund gibt
- eine Aufgabenbeschreibung, sofern vorhanden
- interne Leitfäden und Arbeitshinweise für dieses
- Schulungsmaterialien für ebendieses
- falls es dieses (noch) nicht gibt einen Umsetzungsplan, Zeitplan, Budgetplan und Übersicht der Meilensteine, sofern vorhanden
- sofern vorhanden, Konzeptions- oder Strategiedokumente zu dem Thema
- intern bereits vorhandene Evaluierungen, Präsentationen, Auswertungen, Handlungsempfehlungen zu dem Thema“

Sie beziehen sich dabei eine „Erklärung“ des ITZBund zum Thema „CERT“ auf Twitter:

<https://mobile.twitter.com/ITZBund/status/1567769908519342080>

Über Ihren Antrag entscheide ich nach § 1 Abs. 1 S. 1 IFG wie folgt:

- I. Ich lehne Ihren Antrag ab.
- II. Dieser Bescheid ergeht gebührenfrei.

### Begründung

#### Zu I.

Das ITZBund leistet als zentraler IT-Dienstleister des Bundes im Gefahren- bzw. Notfall koordinierende Arbeit und arbeitet hierbei eng mit dem BSI zusammen. Im ITZBund gibt es Arbeitsgruppen, die auf Sicherheits- und Notfälle spezialisiert sind.

Weitere Auskünfte kann ich Ihnen nicht geben, da das Bekanntwerden dieser Informationen gem. § 3 Nr. 1 lit. c IFG nachteilige Auswirkungen auf Belange der inneren und äußeren Sicherheit haben könnte. Das ITZBund zählt zur kritischen Infrastruktur der Bundesrepublik Deutschland. Durch Veröffentlichung der vorhandenen Konzepte, Schulungsdokumente und Strategien zur Gefahren- bzw. Notfallabwehr, würden Informationen offengelegt, die es ermöglichen würden, Angriffsvektoren abzuleiten. Damit würde die Wahrscheinlichkeit eines zielgerichteten Cyberangriffs auf das ITZBund erhöht und eine kritische Infrastruktur dieses Landes unmittelbar gefährdet.

Als zentraler IT-Dienstleister des Bundes setzt das ITZBund vor dem Hintergrund des Fachkräftemangels, vor allem im IT-Sektor, auf vielfältige Werbemaßnahmen. So betreibt das ITZBund auch Kanäle in den sozialen Medien, wie bspw. auf Twitter (<https://twitter.com/ITZBund>), um zielgruppengerechtes Marketing zu platzieren.

Das ITZBund veröffentlicht auf seinen Kanälen in den sozialen Medien seit einiger Zeit Werbepostings mit dem Titel „partytauglich erklärt“. In diesen Postings werden IT-Begriffe, die man auch als IT-ferne Person möglicherweise schon einmal gehört hat, „partytauglich“ in wenigen Worten und unabhängig vom konkreten ITZBund-Bezug erklärt. Das Ziel hierbei ist das Interesse potenzieller Nachwuchskräfte zu wecken. Am 8. September wurde das Akronym „CERT“ erklärt und mit dem Hinweis auf Stellenangebote des ITZBund auf Twitter veröffentlicht. Die Hinweise auf die Stellenangebote des ITZBund stehen generell nicht im direkten Zusammenhang der erklärten IT-Begriffe dieser Werbereihe.

#### Zu II.

Dieser Bescheid ergeht als einfache Auskunft gem. § 10 Abs. 1 S. 2 IFG gebührenfrei.

Rechtbehelfsbelehrung

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch eingelegt werden. Der Widerspruch ist beim Informationstechnikzentrum Bund, Bernkasteler Str. 8, 53175 Bonn einzureichen.

Mit freundlichen Grüßen

Im Auftrag

