Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Marcel Langner
[redacted]

ausschließlich 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

ifg@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 27.02.2021
Geschäftszeichen: BL23 – 010 03 05/ 2021-012
Datum: 22.03.2021

Sehr geehrter Herr Langner,

Auf Ihre Anfrage nach dem Informationsfreiheitsgesetz (IFG) vom 27.02.2021 ergeht folgender

Bescheid

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

Begründung
1.
In Ihrer oben genannten Anfrage nach dem Informationsfreiheitsgesetz (IFG) bitten Sie um Übersendung von Dokumenten aus denen hervorgeht, dass

„...aufgrund vom Zurückhalten von Informationen über die die Konstruktion/ Aufbau/ Architektur von IT Systemen Angriffe verhindert worden sind? Und auch andersherum/Gegenprobe: nicht verhindert worden sind. Falls ja, bitte ich um Übermittlung.“

Des Weiteren bitten Sie um Übersendung von Dokumenten zur „Frage des Kerckoffs'schen Ansatz des Full Disclosure“

Zu Ihrer Anfrage liegen die folgenden Informationen im Sinne des IFG im BSI vor:

- *Im Rahmen von Zertifizierungsverfahren von Produkten wird die Bewertung potentieller Schwachstellen (-hypothesen) für die individuellen Angriffspfade durchgeführt. Hierbei wird bei der Angriffsstärke auch berücksichtigt, ob für den konkreten*

Angriffspfad benötigte Informationen nicht öffentlich verfügbar sind. Es wird für den Angriff jeweils der Worst Case angenommen, das bedeutet, dass etwa die Berechnung mit und ohne verfügbaren Informationen betrachtet wird (entsprechend potentiell längere Identifizierungsphase für die Schwachstelle). Dieses Verfahren wird auf COTS-Produkte, wie auch auf Halbleiter gleichermaßen angewandt. Dieses Vorgehen ist gemäß den Common Criteria – CC – und der hierzu gehörenden Common Evaluation Methodologie – CEM (https://www.commoncriteriaportal.org/cc/). Die Details finden sich in der CEM, Anhang B.4 Calculating Attack Potential, speziell: B.4.2.2 para 2024 zu Knowledge of the TOE.

- *Zulassungsaussagen des BSI werden unter Anwendung von IT-Sicherheitskriterien zur Bewertung der IT-Sicherheit von IT-Produkten getroffen. Die angewandten Kriterien basieren auf den Internationalen ISO Standards ISO 15408 (Common Critiera) und ISO 18045 (Common Evaluation Methodology / CEM).*
  Als Teil der Betrachtungen fließt insbesondere im Rahmen der Schwachstellenanalyse der Aspekt „Wissen über den Prüfgegenstand (TOE)" in die Betrachtungen mit ein. Abhängig von der Art des Prüfgegenstandes und der von ihm zu erbringenden Sicherheitsleistungen spielt dieser Aspekt eine wesentliche Rolle in der Bewertung der Wirksamkeit der implementierten Schutzmechanismen des Produktes. Nach dieser etablierten und weltweit anerkannten Methodik trägt aber eine verringerte Kenntnis über den TOE grundsätzlich dazu bei, Angriffe schwieriger zu machen und das entsprechende Produkt als widerstandsfähig gegen ein bestimmtes Angriffspotential einzuschätzen.
  In diesem Sinne ist die Anwendung der Common Criteria selbst als Beleg dafür zu sehen, dass das Wissen über den Prüfgegenstand einen Einfluss darauf haben kann, potentielle Schwachstellen leichter oder schwerer identifizieren und ausnutzen zu können.
  In vergleichbarer Weise stellen die in der ALC Klasse der Common Critiera definierten Anforderungen sicher, dass ein Zugang zur Produktdokumentation oder zum SourceCode auf nur berechtigte Personen beschränkt werden. Dies soll zum einen gewährleisten, dass nur authorisierte Änderungen stattfinden und zum anderen, dass die Vertraulichkeit der Entwicklungsumgebung für das IT-Sicherheitsprodukt in Bezug zum Geheimhaltungsgrad in angemessener Weise umgesetzt wird. Unzureichende Schutzmaßnahmen in diesem Bereich ermöglichen Angriffe wie z.B. den kürzlich entdecken Solarwinds-Vorfall.
  Das im Rahmen des o.g. Standards der Common Criteria in der Komponente ALC_FLR geprüfte Verfahren des Herstellers zur Behandlung von Schwachstellen in seinem Produkt stellt sicher, dass Schwachstellen gemeldet und schnell behoben werden können.
  Die im Rahmen eines Zulassungsverfahren verwendeten Informationen zum Produkt werden, aufgrund des nationalen

Regelungscharakters der Zulassung, prinzipiell nur verfahrensbezogen zwischen den beteiligten Parteien ausgetauscht. Dies ist zum einen durch Inhaberrechte des Produktherstellers und zum anderen zusätzlich durch anlassbezogene Einstufungen der Inhalte auf Basis der VSA begründet.

- *Hierzu gibt es den Fall Chipkarten des Typ legic Prime. Das Zurückhalten der Information über die verwendete Verschlüsselung hat nicht dazu geführt, dass diese nicht überwunden werden konnten. Ca. 2009 wurde durch Reverse Engineering der Chipkarten das Kryptoverfahren bekannt und im Nachgang die Verschlüsselung über Software „geknackt". Ähnlich für diverse andere Chipkartentypen. Einige Dokumente dazu finden Sie in der Anlage.*
- *Die Nutzung von geheim zuhaltenden Parametern eines Kryptoalgorithmus ist durchaus üblich. So wird in dem BSI-Dokument „Migration zu Post-quanten-Kryptografie", siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html ,geschrieben:*
  „Für Kryptografie auf elliptischen Kurven bringt die Verwendung von geheim gehaltenen Kurvenparametern einen gewissen Schutz gegen Angriffe mit Quantencomputern."

- *Kapitel "Reconnaissance" des MITRE ATT&CK frameworks (https://attack.mitre.org/tactics/TA0043/). Das MITRE ATT&CK framework ist ein weltweit anerkanntes Schema zur Analyse und Bewertung von Cyber-Angriffen. Relevant für Ihre Fragen sind unter anderem folgende Techniken dieses Kapitels:*
  - *T1590: "Gather Victim Network Information", https://attack.mitre.org/techniques/T1590/*
  - *T1592: "Gather Victim Host Information", https://attack.mitre.org/techniques/T1592/*
  - *T1593: "Search Open Websites/Domains", https://attack.mitre.org/techniques/T1593/*
  - *T1594: "Search Victim-Owned Websites", https://attack.mitre.org/techniques/T1594/*
  - *T1596: "Search Open Technical Databases", https://attack.mitre.org/techniques/T1596/*

  Beispiele, wo solche Techniken angewandt wurden, sind:

  - *SUNSPOT: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/ (T1592)*
  - *Winnti: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/ (T1593, T1594)*
  - *https://us-cert.cisa.gov/ncas/alerts/aa20-304a (T1592, T1593)*

- *Es gibt es immer wieder Berichte, dass die Täter ihre Kontrollserver umziehen, wenn darüber berichtet wird. Ein zusammenfassender Artikel dazu: https://www.techradar.com/news/what-happens-when-we-unmask-the-hackers*

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]