Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

[redacted]
13189 Berlin

Nur per E-Mail:
[redacted]**at.de**

Isabell Kruse
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 27.10.2022
Geschäftszeichen: BL 24 – 010 03 05/ 2022-064
Datum: 23.11.2022

Sehr geehrter Her[redacted]r,

zu Ihrer Anfrage nach dem Informationsfreiheitsgesetz (IFG) vom 27.10.2022 ergeht folgender

Bescheid

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

Begründung
1.
In Ihrer oben genannten Anfrage bitten Sie um Übersendung folgender Informationen:

„Laut telefonischer Aussage der Deutsche Telekom GmbH führt das BSI Portscans bei Bürgern durch und meldet diese an die Provider, welche dann dazu verpflichtet sind, diese über "Sicherheitslücken" in Form offener Ports zu informieren.

Bitte teilen Sie mir folgendes mit:

Auf welcher Rechtsgrundlage werden diese Portscans durchgeführt?
Woher bezieht das BSI die zu scannenden IP-Adressen? Werden ganze Blöcke gescannt? Welche?
Welche offenen Ports werden an die Provider gemeldet?

Bitte senden Sie mir folgendes zu:

Sämtliche mit deutschen Providern ausgetauschten Dokumente bezüglich offener Ports bei Privat- und Geschäftskunden (wenn nötig geschwärzt).

Sämtliche anderen mit deutschen Providern ausgetauschten Dokumente, welche eine Mitteilung der Provider an die Kunden zum Ergebnis hatte (wenn nötig geschwärzt).“

a) *Sämtliche mit deutschen Providern ausgetauschten Dokumente bezüglich offener Ports bei Privat- und Geschäftskunden (wenn nötig geschwärzt).*

Die gewünschten Dokumente liegen im BSI nicht vor. Täglich werden automatisiert etwa 10.000 E-Mails mit Informationen zu offenen/verwundbaren Diensten an die Provider gesendet, welche eine Mitteilung der Provider an die Kunden zum Ergebnis haben könnten. Diese E-Mails werden nicht vollständig gespeichert, sodass eine Bereitstellung der entsprechenden E-Mails nicht ermöglicht werden kann. Beispielhaft finden Sie in der Anlage den Text an die Provider für offen erreichbares Telnet.

b) *Sämtliche anderen mit deutschen Providern ausgetauschten Dokumente, welche eine Mitteilung der Provider an die Kunden zum Ergebnis hatte (wenn nötig geschwärzt).*

Die gewünschten Dokumente liegen im BSI nicht vor. Das BSI bittet die Provider lediglich darum "den Sachverhalt zu prüfen und Maßnahmen zur Absicherung der Systeme zu ergreifen bzw. ihre Kunden entsprechend zu informieren."
Die Provider haben keine Meldepflicht gegenüber dem BSI, welche Informationen letztlich "eine Mitteilung der Provider an die Kunden zum Ergebnis hatten".

Bei Ihren weiteren Fragen handelt es sich nicht um eine Anfrage im Sinne des IFG, sondern um ein allgemeines Auskunftsersuchen. Hierzu gebe ich folgende Informationen an Sie weiter, die mir von den Kollegen der Fachseite übermittelt wurden:

Auf welcher Rechtsgrundlage werden diese Portscans durchgeführt?
Woher bezieht das BSI die zu scannenden IP-Adressen? Werden ganze Blöcke gescannt? Welche?

Das BSI führt keine Scans nach offenen Ports bei Bürgern durch.

Als nationales CERT erhält CERT-Bund täglich von seinen Partnern und weiteren vertrauenswürdigen externen Quellen (zum Beispiel Shadowserver, Team-Cymru oder Spamhaus) eine Vielzahl von Informationen zu Sicherheitsvorfällen und schweren Schwachstellen in Bezug auf IT-Systeme in Deutschland. Dies umfasst unter anderem Informationen zu Systemen, welche mit hoher Wahrscheinlichkeit mit einem Schadprogramm infiziert sind, offen aus dem Internet erreichbare Systeme, welche kritische Sicherheitslücken aufweisen, sowie offene Server-Dienste, welche für DDoS-Reflection-Angriffe gegen Systeme Dritter missbraucht werden können bzw. bereits aktiv missbraucht wurden.

Informationen zu den Reports sind verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/cert-bund-reports_node.html

Welche offenen Ports werden an die Provider gemeldet?

Die Meldungen basieren nicht auf offenen Ports, sondern auf den dahinterliegenden Diensten. Die folgenden Sachverhalte zu offen erreichbaren Diensten werden an die Provider gemeldet, für einige Dienste wurden entsprechende Beschreibungen auch auf der Seite https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/HowTo/howto_node.html bereitgestellt:

Offene Android-Debug-Bridges
Offene BosMon-Server
Cisco-Geräte mit offen erreichbarer Smart-Install-Funktion
Offen erreichbare Smart-Home-Systeme
Offen erreichbare Industrie-Steuerungssysteme
Rsync-Server mit offenen Verzeichnissen
Offene Sphinx-Suchserver
Offene/Kompromittierte Ubiquiti-Netzwerkgeräte
Offene DNS-Resolver
NTP-Server mit aktiver 'monlist' Funktion
Offene CHARGEN-Dienste
Offene Elasticsearch-Server
Offen erreichbare IPP-Druckdienste
Offene CLDAP-Server
Offene mDNS-Server
Offene memcached-Server
Offene MongoDB-Server
Offene MQTT-Dienste
Offene MS-SQL Browserdienste
Offene NetBIOS-Namensdienste

Offene Portmapper-Dienste
Offen erreichbare RDP-Dienste
Offene Redis-Server
Offene SNMP-Dienste
Offene SSDP-Dienste
Offene Telnet-Server

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

Isabell Kruse