Bundesamt
für Sicherheit in der
Informationstechnik

[redacted]hationstechnik, 55133 Bonn

Bundesministerium für Gesundheit
Referat 512
Rochusstraße 1
53123 Bonn

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 06
53133 Bonn

Tel. +49 228 99 9582-[redacted]
Fax +49 228 99 10 9582-[redacted]

referat-di24@bsi.bund.de

poststelle@bsi-bund.de-mail.de

www.bsi.bund.de

Betreff: Pentest von SORMAS und [redacted]

Bezug:
Datum: 24.05.2022
Anlage: 1) E20214054_BSI_SORMAS.v1.0
Anlage: 2) [redacted]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde gebeten, eine Sicherheitsanalyse der Anwendung SORMAS durchzuführen. SORMAS ist eine frei verfügbare Software, die im Rahmen der Pandemiebekämpfung in Deutschland für die Gesundheitsämter angeboten wird. Aus diesem Grund wurde der Kern der Anwendung um diverse Funktionalitäten erweitert. Unter anderem sind daher die Anwendungen von [redacted] und [redacted] integriert worden. Im Zeitraum vom 26.10.2020 bis zum 13.11.2020 und im Zeitraum vom 18.01.2021 bis 12.02.2021 führte das BSI bereits Sicherheitsanalysen der Anwendungen SORMAS, [redacted] durch. Diese Analyse umfassten sowohl Code-Reviews, als auch Penetrationstests. Basierend auf den bisherigen Bewertungen und den Untersuchungen von SORMAS und [redacted] im Zeitraum vom 25.04.2022 bis zum 13.05.2022 finden sich in den folgenden Abschnitten die Einschätzungen des BSI zum Sicherheitsniveau dieser Anwendungen.

1. Ergebnisse des Code-Reviews und Penetrations-Testings von SORMAS

Im Rahmen der Untersuchung von SORMAS wurde ein vollständiger Penetrationstest der Web-Anwendung und des dazugehörigen Hintergrundsystems vorgenommen. Durch die durchgeführten Penetrationstests und Quelltextanalysen konnten geringe bis mittelschwere Schwachstellen identifiziert werden. Da die getestete Anwendung Daten verarbeitet, die als sensibel und vertraulich zu bewerten sind, müssen diese Schwachstellen zeitnah behoben werden.
Eine genaue Beschreibung der Schwachstellen ist in Anlage 1 zu finden.

[redacted]

[redacted]

Fazit

Auf der Grundlage der vom BSI durchgeführten Untersuchungen kann das BMG einem produktiven Betrieb der Systemlandschaft von SORMAS und [redacted] im Hinblick auf die Aspekte der IT-Sicherheit grundsätzlich zustimmen, sofern mindestens die in den vorhergehenden Abschnitten erwähnte hoch prioritäre Schwachstelle zeitnah und angemessen mitigiert wird und es für die verbleibenden Schwachstellen ein angemessener Mitigationsplan vorliegt.

Im Auftrag

[redacted]