Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik, 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, [redacted]

Bezug: Pentest BSI SORMAS
Datum: 13.11.2020

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde darum gebeten, eine Sicherheitsanalyse der Anwendung SORMAS durchzuführen.
SORMAS ist eine frei verfügbare Software, die im Rahmen der Pandemiebekämpfung in Deutschland für die Gesundheitsämter angeboten werden soll. Dabei wurde der Kern der Anwendung um diverse Funktionalitäten erweitert, um den Anforderungen an das aktuelle Einsatzszenario gerecht zu werden. Unter anderem sind daher die [redacted] Die Tests sollten sich daher sowohl auf die Anwendung SORMAS selbst, aber im speziellen auch auf die Schnittstellen zwischen den einzelnen Modulen konzentrieren. Der Testzeitraum lief vom 26.10.2020 bis zum 13.11.2020.

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. Während der Untersuchung konnten verschiedene Schwachstellen identifiziert werden. Diese stellen ein Risiko für die gesamte Sicherheit der Applikation dar. Da die getestete Anwendung Daten verarbeitet, die als sensibel und vertraulich zu bewerten sind, müssen identifizierte Schwachstellen mit hohem Schadenspotential vor dem produktiven Betrieb des Systems behoben werden.
Dies betrifft vor allem folgende Schwachstellen:

- Blind SQL Injection (Anlage 1, Kapitel 5.3.3)
- Stored Cross Site Scripting (Anlage 1, Kapitel 5.3.2).

Alle weiteren bisher nicht behobenen Schwachstellen geringerer Kritikalität sollten ebenfalls in naher Zukunft behoben werden. Eine genaue Beschreibung der Schwachstellen ist in Anlage 1 zu finden.

[redacted]

Fazit

Auf der Grundlage der vom BSI durchgeführten Untersuchungen kann das BMG einer produktiven Inbetriebnahme der Systemlandschaft von SORMAS, [redacted] im Hinblick auf die Aspekte der IT-Sicherheit zustimmen, sofern die in den vorhergehenden Abschnitten aufgeführten und zum Zeitpunkt der Inbetriebnahme zu beseitigenden Mängel behoben und erfolgreich getestet sind.

Im Auftrag

[redacted]
Referatsleiter DI24