EMPFEHLUNG: IT IN CORONA-TESTZENTREN

Informations- und Datensicherheit von Corona-Testzentren

„Mehrere Tausend persönliche Daten aus Corona-Testzentren öffentlich im Internet einsehbar." Diese Schlagzeile war in den letzten Tagen und Wochen mehrfach in den Medien zu lesen.

Das BSI nimmt diese aktuelle Berichterstattung zum Anlass, um insbesondere aufgrund der Sensibilität dieser Gesundheitsdaten, die Betreiber und Dienstleister der Corona-Testzentren erneut für das Thema Informations- und Datensicherheit zu sensibilisieren.

1 Ziel des Dokuments

Mit den nachfolgenden Informationen möchte das BSI über die häufigsten dem BSI bekannten Schwachstellen von Web-Anwendungen bei Corona-Testzentren informieren und Empfehlungen zur Behebung dieser Schwachstellen liefern. Diese Informationen bieten jedoch lediglich einen ersten Schritt in Richtung Informations- und Datensicherheit. Für einen vollumfänglichen Schutz der bei Corona-Testzentren erhobenen Datensätze sind weitere Maßnahmen (siehe 4 Weiterführende Informationen) umzusetzen.

2 Häufige Schwachstellen

Bisher wurden dem BSI die nachfolgenden Schwachstellen bei den Betreibern der Corona-Testzentren bekannt:

Fehler in der Zugriffskontrolle[1]**:** Die Übermittlung der Testergebnisse wird je nach Testzentrum unterschiedlich gehandhabt - teilweise wird das Ergebnis per E-Mail verschickt, teilweise erfolgt der Abruf über ein Webportal. Beim Abrufen über ein Webportal konnte beobachtet werden, dass der dafür benötigte Link häufig eine inkrementierende Identifikationsnummer für spezifische Testvorgänge beinhaltete. Durch einfaches Heraufzählen dieser Nummern war es immer wieder möglich, Testergebnisse sowie persönliche Daten anderer Probanden einzusehen. Wird das Testergebnis per E-Mail verschickt, erfolgt die Zusendung häufig über ein passwortgeschütztes PDF-Dokument. Hier kommen mitunter zu kurze Passwörter zum

1 https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control

Einsatz - z.T. bestehend aus sechs oder weniger Zeichen. Die Identifikation dieser Passwörter ist Angreifern innerhalb kurzer Zeit mittels trivialer Methoden möglich.

Verlust der Vertraulichkeit sensibler Daten[2]: Wiederholt kam es im Corona-Test-Umfeld zu Offenlegungen von sensiblen Daten. In einem Fall konnten API-Schlüssel[3] direkt im Rahmen des Buchungsprozesses für einen Testtermin eingesehen werden. In einem anderen Fall gelang dies über die Nutzung der vom Browser mitgelieferten Entwickler-Tools. Im Folgenden konnten API-Aufrufe durchgeführt werden, die Zugriff auf persönliche Daten von Probanden, Testtermine und Testergebnisse ermöglichten.

3 Empfehlungen

Die Sicherheit eines jeden Webangebots resultiert – wie grundsätzlich bei Software – besonders aus der sorgfältigen Berücksichtigung sicherheitsspezifischer Anforderungen im Rahmen der Entwicklung (Security by Design). Die Einhaltung dieses Prinzips durch den Hersteller sollte bei der Auswahl der eingesetzten Software als entscheidungsleitend angesehen werden.

Zudem sollten gem. Datenschutz-Grundverordnung (DSGVO) durch die Corona-Testzentren lediglich Daten erhoben werden, die für die Durchführung des Testprozesses unverzichtbar sind (Grundsatz der Datensparsamkeit).

Das Open Web Application Security Project (OWASP) analysiert regelmäßig die größten Sicherheitsrisiken webbasierter Anwendungen und veröffentlicht diese in den OWASP Top 10.[4] Diese Liste ist in der jeweils aktuellen Fassung zu berücksichtigen und den dort aufgeführten Gefährdungen mit geeigneten Maßnahmen dauerhaft zu begegnen.

Um bereits bestehende Webanwendungen auf ein definiertes Sicherheitsniveau zu bringen sollten mindestens die folgenden Schritte umgesetzt werden:

Absicherung der Web-Infrastruktur

- Netzwerk absichern
  Eine Absicherung des Netzwerkes unter anderem durch Firewalls ist prinzipiell zu empfehlen.
- Serverhärtung durch Minimalisierung
  Eine Minimalisierung der Dienste auf den betriebenen Servern ermöglicht die Verringerung der Angriffsfläche und somit eine Härtung der Server gegen Angriffe.
- Überwachen von Protokolldateien
  Durch die Überwachung von Protokollen können Angriffe frühzeitig erkannt und mitigiert werden.
- Patchmanagement
  Durch regelmäßiges Aktualisieren der Software werden Schwachstellen zeitnah geschlossen.

Bestandsaufnahme

- Vollständige Sicherheitsanalyse der gesamten Webanwendung und ihrer Komponenten
  Eine einzige unsichere Komponente kann die Sicherheit der Gesamtanwendung und Systeme gefährden. Deshalb sollte die Webanwendung als Ganzes betrachtet werden.

2 https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure
3 API steht für Application Programming Interface und bezeichnet eine Programmierschnittstelle.
4 https://owasp.org/www-project-top-ten/

Sicherheitsanalyse / Penetrationstest

- Untersuchung der Anwendung auf das Vorhandensein von Schwachstellen
  Dadurch können einfache Schwachstellen schnell gefunden und beseitigt werden.

Risikoanalyse

- Risikoübernahme und Einschätzung
  Sofern bestimmte Schwachstellen/Probleme nicht behoben werden können, ist eine Risikoanalyse durchzuführen.

Festlegung und Umsetzung von Schutzmaßnahmen

- (Grundschutz-)Maßnahmen und Best Practices anwenden

Etablierung geeigneter Sicherheitskontakte[5]

- Entsprechende Sicherheitskontakte sollten beispielsweise auf der Webseite bekanntgegeben werden, um direkt von Sicherheitsforschenden über Schwachstellen informiert zu werden.

4 Weiterführende Informationen

Weiterführende Informationen zur Sicherheit von Webanwendungen sind unter den nachfolgenden Links zu finden.

Übersicht Webanwendungen:
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Web-Anwendungen/webanwendungen_node.html

IT-Grundschutz (u.a. Bausteine APP.3.1 Webanwendungen und CON.10 Entwicklung von Webandwendungen):
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Leitfaden zur Entwicklung sicherer Webanwendungen. Empfehlungen und Anforderungen an die Auftragnehmer (2013):
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftragnehmer.pdf

Sicherheit von Webanwendungen - Maßnahmenkatalog und Best Practices:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec.pdf?

Übersicht mit Sicherheitshinweisen des LfDI BW für Testzentren:
https://www.baden-wuerttemberg.datenschutz.de/pandemie-bekaempfung-datenschutz-in-testzentren/

OWASP Top 10 -2017 Die 10 kritischsten Sicherheitsrisiken für Webanwendungen (Deutsche Version 1.0):
https://wiki.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf

Handhabung von Schwachstellen:
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.html

5 Die Nutzung bekannter Standards wie beispielsweise https://securitytxt.org wird empfohlen.

Pentesting:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/IS-Rev/Liste-IT-Sicherheitsdienstleister/liste-it-sicherheitsdienstleister_node.html

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Leserinnen und Lesern an **service-center@bsi.bund.de** gesendet werden.