Mindestanforderungen an Teststellen zur Durchführung von Teststellen auf das Vorliegen des Coronavirus SARS-CoV-2

Für den Betrieb einer Teststelle sind infektions- und arbeitsschutzrechtliche sowie medizinprodukterechtliche Vorschriften zu beachten. Zudem bestehen Anforderung an die Zuverlässigkeit und Angaben zur vorhandenen Testkapazität.

Im Folgenden sind die Mindestanforderungen zusammengefasst.

1. **Test- und Hygienekonzept:**

- Es liegt ein schriftliches Test- und Hygienekonzept vor.
- Das Test- und Hygienekonzept berücksichtigt die geltenden Arbeitsschutzregeln, insbesondere in Bezug auf SARS-CoV-2,

  a) die Empfehlungen des Robert Koch-Instituts zum Infektionsschutz sowie die
  b) Schutzvorschriften gemäß der Sächsischen Corona-Schutzverordnung und der
  c) Allgemeinverfügung über die Anordnung von Hygieneauflagen des Sächsischen Staatsministeriums für Soziales und Gesellschaftlichen Zusammenhalt
  d) Arbeitsschutzstandards des Bundesministeriums für Arbeit und Soziales, insbesondere in Bezug auf SARS-CoV-2
  e) Medizinprodukte-Betreiberverordnung und Medizinprodukte-Abgabeverordnung
  f) Coronavirus-Testverordnung

2. **Infektions- und arbeitsschutzrechtliche Mindestanforderungen bzgl. räumlichen Gestaltung und Durchführung von Testungen**

- Die Bürger werden mittels entsprechender Beschilderung im Eingangsbereich über einzuhaltende Hygieneregeln und die maximale Personenanzahl belehrt. Es wird darauf hingewiesen, dass die Testung nur für asymptomatische Personen erfolgt und symptomatische Personen an den Hausarzt verwiesen werden.
- Handdesinfektionsmittelspender mit geeignetem Desinfektionsmittel stehen bereit.
- Hinweise auf das Tragen einer medizinischen Mund-Nasen-Bedeckung für Patienten und Dienstleister ist gegeben (keine Visiere): medizinische Masken/ FFP2-Masken
- Besucherströme werden so gelenkt, dass Ansammlungen von Menschen oder eine Unterschreitung des Mindestabstands verhindert werden. Dazu können z. B. Einbahnstraßensysteme genutzt werden.
- Der Mindestabstand von 1,5 Meter wird zwischen Personen in jede Richtung eingehalten. Dafür sind Markierungen am Boden angebracht.
- Die Wegebeziehungen des Personals werden berücksichtigt.

- Es ist ein Lüftungskonzept vorhanden. Es wird für eine ausreichende und regelmäßige Lüftung, ggf. unter Zuhilfenahme einer Klimaanlage in fensterlosen Räumen, gesorgt. Eine Querlüftung mit Frischluft wird mind. alle 30 Minuten für eine Dauer von 5 Minuten empfohlen.
- Differenzierung der Wartebereiche vor und nach der Testung und ggf. für Kontaktpersonen.
- Regelmäßige Reinigung und Desinfektion der Toiletten, Waschbecken, Türgriffe und der wischbaren Böden. Die Oberflächendesinfektion erfolgt mit begrenzt viruzidem Desinfektionsmittel, vorgetränkten Tüchern und nicht mit Sprühdesinfektion.
- Das Personal wird über die Umsetzung des Test- und Hygienekonzeptes regelmäßig belehrt. Die Belehrungen sind schriftlich hinterlegt.
- Bei der Durchführung des Tests wird persönliche Schutzausrüstung getragen (FFP2 Masken, Handschuhe, Schutzbrillen/Visiere, Schutzkittel).
- Ein Handwaschplatz mit Flüssigseife und Einmalhandtüchern steht für das Personal zur Verfügung.
- Die Trennung Pausenbereich / Umkleidebereich / Arbeitsbereich ist gewährleistet.
- Die adäquate und ordnungsgemäße Entsorgung des Verbrauchsmaterials ist gesichert (stabile, reißfeste, fest verschlossene Müllbeutel in die Restmülltonne geben).

3. Medizinproduktrechtliche Anforderungen

- Die verwendeten Antigen-Schnelltests entsprechen den durch das Paul-Ehrlich-Institut in Abstimmung mit dem Robert Koch-Institut festgelegten Mindestkriterien für Antigentests.
- Die Testung wird nur durch fachlich geeignetes Personal durchgeführt. Es wird ausreichend Personal für die Durchführung der Testung eingeteilt und eine fachliche Leitung bestellt.
- Es ist sichergestellt, dass die mit der Testung betrauten Kräfte, die nicht über eine medizinische oder pflegefachliche Ausbildung verfügen, die notwendigen Kenntnisse und Erfahrungen in der Anwendung des Tests verfügen. Dazu eignet sich insb. die ärztliche Schulung im Sinne des § 12 der TestV.
- Für die Leistungserbringung nach § 4b TestV ist der Einsatz von geeigneten pflegerischem oder medizinisches Fachpersonal gemäß § 5 a IfSG erforderlich.
- Die Durchführung und Auswertung erfolgt entsprechend der Herstellerangaben des Test-Kits und muss allen testenden Personen bekannt sein.
  Insbesondere sind zu beachten:
  - vorgeschriebene Reihenfolge und Ablauf zur Test-Anwendung
  - Bedingungen zur Lagerung

- Temperatur der Tests bei Anwendung (Raumtemperatur!)
- Haltbarkeit der Tests
- vom Hersteller empfohlene Testkontrollen mittels Kontrollflüssigkeit
- Bedingungen zur Auswertung des Tests (Kontrollbalken, Zeitintervall) (§ 4 MPBetreibV)

4. Mindestanforderungen zur Zuverlässigkeit der Durchführung und Mitteilung der Testkapazität

- Die Anzahl der vorgehaltenen Testplätze, der testenden Personen und der Öffnungszeiten ist benannt. Bei mehreren Standorten in einer Gebietskörperschaft müssen diese Aussagen pro Standort erfolgen.
- Die Teststelle ist für die Allgemeinheit zugänglich und bietet zu vereinbarten Öffnungszeiten (auch in den Nachmittagsstunden oder am Wochenende) Testmöglichkeiten an.
- Auf der Grundlage der Testplätze, der Anzahl der testenden Personen und der Öffnungszeiten werden dem Gesundheitsamt eine max. Anzahl von monatlichen Tests mitgeteilt.
- Bei einer temporären Ausweitung der Testplätze oder Einrichtung von mobilen Teststellen, wie sie bspw. vor Großveranstaltungen möglich sein kann, werden die erhöhten Testkapazitäten und die Hygienekonzepte der mobilen Stationen vorher beim Gesundheitsamt beantragt.
- Alle zu testenden Personen erhalten vorab der Testung Informationen über diese. Die Informationen hängen in der Einrichtung aus. Das Einverständnis der zu testenden Personen oder von deren Vertreter/-in in die Testung liegt dokumentiert vor.
- Das Testergebnis wird in schriftlicher oder digitaler Form übergeben. Ab dem 1. August 2021 wird das Testergebnis auch über die Corona-Warn-App mitgeteilt.
- Die Testungen werden entsprechend den Vorgaben zur Dokumentation und Abrechnung der Kassenärztlichen Bundesvereinigung fortlaufend dokumentiert (Aufbewahrung für Abrechnung bei der KV bis 31.12.2024, auch Daten zur Prüfung des Anspruchs auf Testung, Testdurchführung, für Ausstellung des Testzertifikats notwendigen Daten, damit auch personenbezogene Daten).
- Monatlich und standortbezogen erfolgt die Meldung der durchgeführten Bürgertestungen nach § 4a TestV und der Gesamtanzahl der positiven Tests an das zuständige Gesundheitsamt per E-Mail an gesundheitsamt.stabsstelle@stadt-chemnitz.de.
- Positive Befunde werden unverzüglich durch das digitale Meldeportal an das zuständige Gesundheitsamt übermittelt. Alternativ zum digitalen Meldeportal der Stadt Chemnitz besteht die Möglichkeit zur Nutzung des Deutschen Elektronischen Melde- und Informationssystems für den Infektionsschutz (DEMIS).

- Bei positivem Antigenschnelltest werden die getesteten Personen auf die Pflicht zur Nachuntersuchung mittels PCR-Test hingewiesen und über die Pflicht zur Absonderung hingewiesen. Hilfestellung geben die Hinweise auf https://www.coronavirus.sachsen.de/downloads-10288.html.

5. Weitere Hinweise

- Die Beendigung bzw. Unterbrechung des Testangebots wird dem Gesundheitsamt und der Kassenärztlichen Vereinigung Sachsen unverzüglich mitgeteilt.
- Eine Beschilderung zum Auffinden der Teststelle ist vorhanden.
- Bei externen oder mobilen Testungen in Einrichtungen etc. sind die vorstehenden Anforderungen ebenfalls entsprechend sicherzustellen.
- Informationen sind mehrsprachig vorhanden.
- Bürgertestungen nach § 4a dürfen nicht zur Erfüllung von Testpflichten der Arbeitgeber oder im Rahmen der schulischen Testung erfolgen.
- Im Rahmen des Betriebs der Teststelle als weiterer Leistungserbringer nach § 6 Abs. 1 Nr. 2 ist die Verarbeitung personenbezogener Daten erforderlich, darunter auch besonderer Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, nach Art. 9 Datenschutz-Grundverordnung (DS-GVO). Die Teststelle ist dafür Verantwortlicher (Definition siehe Art. 4 Nr. 7 DS-GVO) im Sinne des Datenschutzrechts. Die Einhaltung aller einschlägigen datenschutzrechtlichen Bestimmungen wird hiermit versichert.
- Das Personal ist über den Datenschutz und die Schweigepflicht belehrt.
- Die Empfehlungen zur Informations- und Datensicherheit von Corona-Testzentren des Bundesamtes für Sicherheit in der Informationstechnik vom 28.06.2021 werden umgesetzt. (siehe Anlage)

Anlage

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Veröffentlichungen zur Cyber-Sicherheit

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.