Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Abschlussbericht Projekt MaSiGov – Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Apps und Webportalen

Eine aktuelle Marktanalyse und IT-Sicherheitsbetrachtung

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.7	20.09.2022	BSI & Secuvera GmbH	Erstversion
0.8	24.11.2022	BSI & Secuvera GmbH	Ergebnisse und Erkenntnisse
0.9	30.01.2023	BSI & Secuvera GmbH	Kommentierungsentwurf
0.95	17.02.2023	BSI & Secuvera GmbH	Einarbeitung Feedback
1.0	08.03.2023	BSI	Fertigstellung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
masigov@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Ausgangslage und Hintergrund

Durch das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz) vom 14.08.2017 sind Bund und Länder verpflichtet, bis spätestens 30.12.2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten (§ 1 Abs. 1 OZG) [1]. Ein Beispiel für eine Verwaltungsleistung, die bisher physisch vor Ort stattfinden musste, ist der Antrag zur Ummeldung des Wohnortes, für den sich der Bürger zukünftig nicht mehr bei der Behörde einfinden muss, sondern diesen von zu Hause aus vornehmen kann.

Im Rahmen von digitalisierten Antragsverfahren müssen Bürgerinnen und Bürger häufig Daten von hoher Empfindlichkeit angeben. Am Beispiel der Ummeldung wären dies u. a. Wohnanschriften und Angaben aus dem Personalausweis. Anlässlich der Frist zur Umsetzung des OZG sowie der großen Anzahl an betroffenen Leistungen haben viele Kommunen und Länder bereits damit angefangen, die Anforderungen des OZG in ihre bestehenden Portale zu integrieren oder neue Portale zielgerichtet zu entwickeln. Dementsprechend existiert derzeit eine große Vielfalt an Lösungen, die auf unterschiedlichsten Ansätzen beruhen und zusätzlich um weitere nützliche Funktionen ergänzt werden. Infolge der Interoperabilität des Portalverbunds steigt somit die Komplexität für eine sichere Lösung weiter.

Das Projekt MaSiGov hat von Januar 2022 bis Januar 2023 stattgefunden. Es dient als Grundlage, um im Umfeld der vielfältigen Lösungen der OZG-Portale im Hinblick auf IT-Sicherheit handlungsfähig zu sein und die Entwickler sowie die Betreiber der unterschiedlichen Portallösungen dabei zielgerichtet unterstützen zu können. Die im Rahmen des Projekts gewonnenen Erkenntnisse sollen zum einen zeigen, wie Portallösungen verbessert werden können. Zum anderen sollen dazu Hilfestellungen in Form von Handlungsempfehlungen und Technischen Richtlinien erarbeitet und bereitgestellt werden.

1.2 Zielsetzung und Aufbau der Studie

Ziel des Projekts ist es, das Potenzial und die Schwachstellen von aktuell auf dem Markt befindlichen Portallösungen im E-Government-Kontext zu identifizieren und die gewonnenen Erkenntnisse in Technische Richtlinien und Handlungsempfehlungen einfließen zu lassen.

Um die genannten Ziele zu erreichen, wurden im Projektverlauf die zwei folgenden Schritte durchgeführt:

1. Eine Marktanalyse, die einen Überblick über die entwickelten und eingesetzten Lösungen für Webportale und Apps im E-Government-Kontext gibt, sowie
2. Schwachstellenanalysen von ausgewählten Portalen im Einvernehmen mit den Produktverantwortlichen, bei denen die Portale gezielt angegriffen werden, um IT-sicherheitsrelevante Schwachstellen zu finden.

2 Projektauftrag

2.1 Vorgehen

Das Projekt ist in mehrere Teilprojekte bzw. Projektphasen untergliedert worden. Zunächst wurde eine Marktanalyse durchgeführt, um einen Überblick über aktuelle Produkte und deren eingesetzte technische Lösungen zu erhalten. Die Ergebnisse der Marktanalyse wurden anschließend anhand von spezifischen Auswahlkriterien strukturiert und ausgewertet, um so später eine Vergleichbarkeit und damit aussagekräftige Ergebnisse erzielen zu können.

Die Auswahl an Portalen, die anhand definierter Kriterien getroffen wurde, wurde im nächsten Schritt durch die secuvera GmbH einem Penetrationstest unterzogen. Hierfür wurden sowohl ein Angriffskatalog als auch für jedes einzelne Portal ein spezifischer Durchführungskatalog festgelegt. Der Durchführungskatalog diente während des Penetrationstests als Testplan, der die einzelnen Prüfungen beschreibt und so als Grundlage für eine nachvollziehbare und wiederholbare Prüfung eingesetzt werden konnte.

Die Ergebnisse des Penetrationstests wurden anschließend in einem Ergebnisbericht, der für jedes Portal einzeln angefertigt wurde, zusammengefasst. Anhand dieser Analyse konnten Erkenntnisse für eine Handlungsleitfaden gewonnen werden, der nach Abschluss des Projekts erstellt wird. Des Weiteren konnten die Ergebnisse in die Technische Richtlinie BSI TR-03172 Portalverbund eingearbeitet werden.

2.2 Definitionen

2.2.1 Definition Portal

Ein Portal (oder auch: Webportal) bezeichnet eine Anwendung, die von einem Webserver ausgeführt wird. Ein Benutzer kann eine solche Anwendung beispielsweise in einem Browser öffnen und verwenden. Zur Navigation innerhalb und zur Bedienung des Webportals steht dem Benutzer ein sogenanntes Front-End (auch: Benutzeroberfläche) zur Verfügung, das dem Benutzer sowohl ermöglicht, Daten abzurufen, als auch, Eingaben zu machen (z. B. Befüllung von Datenfeldern oder Upload von Unterlagen). Über dieses Front-End werden dem Benutzer gesammelte Informationen zu einem oder mehreren spezifischen Themen zur Verfügung gestellt.[1] Während für das Front-End klassische Technologien wie HTML und CSS zum Einsatz kommen, werden Hintergrundprozesse wie beispielsweise Datenbankabfragen durch SQL, verschiedene Frameworks und dazugehörige Implementierungen ermöglicht.

Im Projekt MaSiGov wurden nur Webportale und die von diesen direkt angesprochenen Schnittstellen untersucht.

Der Fokus des Projekts lag auf der Untersuchung von Service- oder Kommunalportalen. Der Begriff „Serviceportale“ beschreibt die E-Government-Portale von Bundesländern. Kommunalportale sind E-Government-Portale der einzelnen Kommunen.

Im Zuge des in Kapitel 1 eingeführten Beispiels bedeutet das Folgendes: Das Ausfüllen des Antrags „Ummeldung des Wohnsitzes“ durch den Benutzer erfolgt mithilfe einer Antragsstrecke. Dies geschieht in einem Webportal und soll daher im Projekt MaSiGov betrachtet werden.[2]

[1] Im Projekt MaSiGov entspricht dies OZG-Leistungen.

[2] Hinweis: Die Entgegennahme des Antrags sowie die Interpretation der eingegebenen Daten ist dagegen kein Teil dieses Projektes.

2.2.2 Definition App

Eine App wurde im Rahmen des Projekts als eine Anwendung definiert, die vor Verwendung durch den Nutzer auf einem mobilen Gerät installiert werden muss und auch nur dort genutzt werden kann. In der Regel erfolgt dies auf einem Smartphone oder Tablet mithilfe eines sogenannten App-Stores.[3] Desktop-Apps werden im Rahmen dieses Projekts dagegen nicht berücksichtigt.

Die direkte Interaktion durch den Benutzer sowie die Bereitstellung von Informationen erfolgt ebenfalls über ein Front-End. Native Apps benötigen im Gegensatz zu den Webportalen keinen Browser. Sie laufen daher vollumfänglich auf dem mobilen Endgerät. Progressive Apps, die sich als Kompromiss zwischen responsiver Webseite und nativer App beschreiben lassen, verwenden für den Aufruf ebenfalls einen Browser. Daher bieten sie keinen zusätzlichen Erkenntnisgewinn gegenüber Webportalen. Aus diesem Grund sollen im Rahmen des Projekts MaSiGov lediglich native Apps betrachtet werden.

2.3 Projektteam

Das Projektteam bestand aus Mitarbeiterinnen und Mitarbeitern des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Bonn und Freital sowie der secuvera GmbH in Gäufelden.

Das BSI ist die zentrale, unabhängige und neutrale Stelle zu Fragen der IT-Sicherheit. Als Cyber-Sicherheitsbehörde des Bundes gestaltet das BSI Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion. Mitarbeiterinnen und Mitarbeiter des BSI aus den Referaten DI 15 „eID-Lösungen für die digitale Verwaltung“ und DI 27 „Cyber-Sicherheit bei der Umsetzung des Onlinezugangsgesetzes“ übernahmen die Projektleitung des Projekts „Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Webportalen und Apps.“

Die secuvera GmbH ist ein vom BSI zertifizierter IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung sowie für die Durchführung von IS-Penetrationstests. Im Rahmen der Zertifizierung wurden Zuverlässigkeit und Unabhängigkeit sowie Fachkompetenz und Qualität der Dienstleistung geprüft und bestätigt. Damit wurde von unabhängiger Stelle die Vertrauenswürdigkeit und Kompetenz der durch secuvera erbrachten IT-Sicherheitsdienstleistungen nachgewiesen.

[3] Eine weitere Möglichkeit besteht – unabhängig durch einen App-Store – durch die Installation von apk-Dateien.

3 Marktübersicht

In einem ersten Projektteil sollte der Markt der im Einsatz befindlichen E-Government-Apps und Webportale auf Kommunal- und Landesebene betrachtet werden, um die aktuelle Vielfalt an Umsetzungen, Produkteigenschaften und Anforderungen abzubilden und zu verstehen. Aufgrund der stark unterschiedlichen Beschaffenheit der Produkte selbst, z. B. der Bereitstellung der Produkte, wurde ein unterschiedliches Vorgehen für die Marktanalyse zwischen Apps auf der einen Seite und Webportalen auf der anderen Seite festgelegt.

3.1 Produktkategorie Apps

3.1.1 Internet-Recherche

Die Marktanalyse von Apps für mobile Endgeräte fand zwischen Frühjahr 2021 und Frühjahr 2022 statt. Ziel war es, den bestehenden Markt an relevanten Apps zu erfassen und etwaige Entwicklungen zu beobachten. Hierfür wurden vorhandene Apps identifiziert sowie ihre Funktionalitäten festgehalten und kategorisiert. Nach 12 Monaten wurden die Apps erneut auf ihre Funktionalität überprüft. Auf Basis der im Frühjahr 2022 vorhandenen Funktionalitäten wurde die Relevanz der gefundenen Apps für das Projekt beurteilt.

Die Bereitstellung von Apps für mobile Endgeräte erfolgt in der Regel über sogenannte App-Stores als gängige Vertriebsplattform. Diese App-Stores wurden methodisch auf Apps mit Bezug zu den Verwaltungen von Kommunen und Ländern durchsucht. Hierzu wurde u. a. nach einschlägigen Begriffen wie „Rathaus“, „Verwaltung“ und „Bürgerservice“ gesucht. Zusätzlich wurde für jede gefundene App untersucht, ob der Anbieter weitere Apps mit ähnlicher Aufgabe bereitstellte. Wurden von einem Anbieter mehrere Produkte gefunden, so wurden diese ebenfalls mit aufgenommen. In einem zusätzlichen Schritt fand zudem ein Vergleich der gefundenen Produkte eines Anbieters durch Kriterien wie „Auftreten“ und „Funktionsumfang“ statt.

Die Features der Apps wurden anhand der in dem jeweiligen Shop bereitgestellten Informationen, wie Beschreibung und Screenshots der App-Oberfläche, erhoben. Stichprobenartig sowie bei unklarer Sachlage fand eine tiefere Recherche zu den Features der Apps statt. Diese erfolgte, sofern vorhanden, auf Informationsseiten zur jeweiligen App im Internet, die von der jeweiligen Verwaltung oder dem Anbieter bereitgestellt worden waren. Zusätzlich fand vereinzelt eine Installation und Ausführung der App auf einem unterstützten mobilen Endgerät mit anschließender Überprüfung des Funktionsangebots statt.

3.1.2 Direktkontakte

Im Rahmen der Marktanalyse fand eine Kontaktaufnahme mit fünf Anbietern und Entwicklern von gefundenen Apps statt. In drei Fällen erfolgte die Kontaktaufnahme bei unklaren Informationen zur technischen Umsetzung oder Funktionalitäten mit OZG-Bezug, in zwei Fällen aufgrund von Alleinstellungsmerkmalen. Bei den Kontakten wurden neben dem aktuellen Funktionsumfang der Apps auch Pläne für die Weiterentwicklungen der Apps inklusive neuer Funktionsbereiche erfragt.

3.1.3 Ergebnis

Insgesamt wurden 206 unterschiedliche Apps von 41 eingetragenen Anbietern identifiziert. Von den gefundenen Apps waren 173 (ca. 84 %) sogenannte White-Label-Lösungen, bei denen ein Produkt von mehreren Stellen genutzt oder nachgenutzt wird. 144 der gefundenen Apps (ca. 70 %) entfielen hierbei auf drei Anbieter, die jeweils 81, 33 und 30 Produkte für einzelne Kommunen bereitgestellt hatten. Für 33 Apps (ca. 16 %) waren individuelle Anbieter ohne weiteres vergleichbares Produkt eingetragen. Die konkrete Aufteilung der Produkte nach Anbietern ist in Abbildung 1 dargestellt. Anzumerken ist hier, dass in einem Fall zwei Versionsstände einer Lösung parallel existierten.

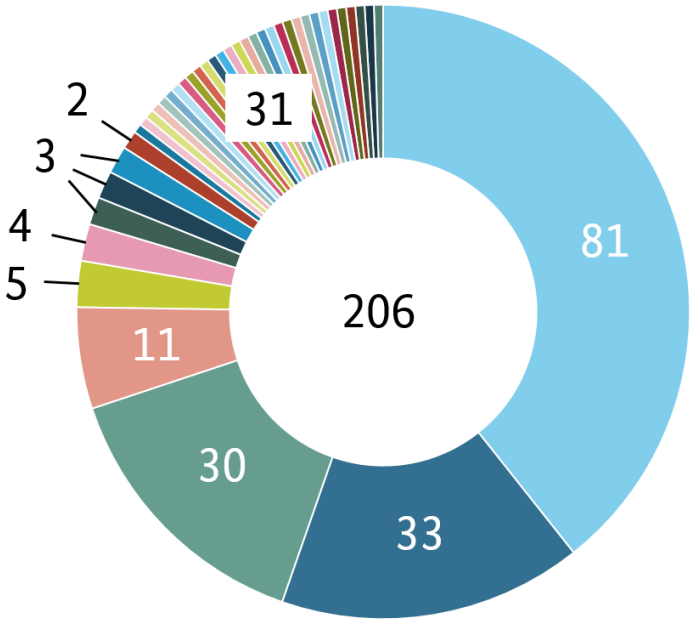

Abbildung 1: Anzahl Apps für mobile Geräte pro Anbieter. Jede Farbe entspricht einem Anbieter

Die Apps konnten in ihrer Funktionsweise grundsätzlich unterschieden werden in native Lösungen und Browserlösungen. Bei nativen Lösungen kann eine Datenverarbeitung oder Speicherung zumindest teilweise innerhalb der App und demzufolge auf den mobilen Endgeräten selbst stattfinden. Bei browserbasierten Lösungen dient die App vorwiegend als Webbrowser, der in großen Teilen das Webportal der Kommune oder des Landes aufruft. Apps, die vornehmlich als Browserlösung fungieren, wurden im Rahmen des Projektes nicht als relevant gewertet, da es sich hier lediglich um eine progressive Webanwendung handelt und daher keine Unterschiede zu einer Browserlösung zu erwarten sind. Die sensiblen Informationen der antragstellenden Person wurden hier vom Dienst des nachgeschalteten Webportals entgegengenommen und verarbeitet. Da die Verarbeitung von sensiblen Daten hier im Webportal erfolgte, wurden diese Apps im Rahmen des Projekts nicht berücksichtigt.

Eine weitere Unterteilung erfolgte im Funktionsumfang der Apps. Dieser konnte in zwei Kategorien unterschieden werden. Die erste Kategorie umfasste Funktionen der reinen Informationsprovision für den Nutzer. Hier erfolgte der Informationsfluss unidirektional von der Verwaltung aus – ohne Eingabe von möglicherweise sensiblen Daten durch den Nutzer. Die Funktionen der Informationsprovision umfassten vornehmlich:

- aktuelle Informationen und Bekanntmachungen der Verwaltung,
- Veranstaltungskalender,
- Ortsdaten von Points of Interest (PoI) im Zusammenhang Tourismus, Amtsadressen sowie Parkplätze,
- Kontaktdaten und Informationen über angebotene Dienste, wie Abfallkalender, ÖPNV und Stellenausschreibungen.

Die zweite Kategorie umfasste Funktionen, in denen eine Eingabe von Daten durch den App-Nutzer möglich war. Die vorgefundenen Funktionen dieser Kategorie bestanden vornehmlich aus:

- Mängelmelder,
- Terminbuchungen,
- Kontaktformulare,
- Feedbackmöglichkeiten.

Zum Zeitpunkt der Erhebung konnte keine App gefunden werden, die eine Antragsstellung von Verwaltungsleistungen nach OZG mit nativer Lösung anbot.

Die Marktanalyse hat gezeigt, dass Apps für mobile Geräte vorrangig für die Informationsprovision genutzt werden. Hierbei zeigte die Mehrzahl der Apps (>80 %) zumindest einen Schwerpunkt auf touristische Aspekte. Ein weiterer Schwerpunkt lag im Nutzen der Mobilität des Smartphones. So bot etwa die Hälfte der Apps die Funktion eines Mängelmelders an, in der z. B. ein Foto eines Missstands, etwa eines überfüllten Abfalleimers, aufgenommen und zusammen mit Informationen zu Ort und Zeit an die Verwaltung übermittelt werden kann.

Die Einbindung von digitalen Verwaltungsleistungen mit OZG-Kontext in Apps ist ein derzeit für die Entwickler aufkommendes und von der Verwaltung gewünschtes Thema. Hierbei existieren bisher lediglich browserbasierte Lösungen. Aus diesem Grund wurde als Resultat der Marktanalyse keine App als Produkt für eine Schwachstellenanalyse gefunden. In den Gesprächen mit Entwicklern zeigte sich jedoch, dass native Lösungen zumindest bei einzelnen Entwicklern in der Planung oder Entwicklung sind, während andere Entwickler bis auf weiteres auf eine Integration von OZG-Leistungen verzichten.

3.2 Produktkategorie Webportale

Im Rahmen des Projekts wurde eine Marktanalyse bereits existierender Webportale auf kommunaler und Landesebene durchgeführt. Als Ergebnis dieses Projektteils war eine Übersicht über Webportale mit Verwaltungsleistungen nach Onlinezugangsgesetz vorgesehen.

Während der Marktanalyse stellte sich heraus, dass bei der Entwicklung von E-Government-Webportalen verschiedene Ansätze verfolgt wurden. Dadurch gab es viele unterschiedliche Lösungen. Beispielsweise fanden sich selbst bei einzelnen Kommunen interne Eigenentwicklungen, wodurch eine Bewertung der Eignung der Webportale für das Projekt erschwert wurde. Zudem waren Informationen zu Strukturen oder Entwicklern von Webportalen öffentlich schwer zugänglich. Um möglichst viele verschiedene Produkte zu identifizieren, wurden unterschiedliche Ansätze verfolgt. Hierbei lag der Fokus auf folgenden Kriterien:

1. Internet-Recherche,
2. Fragebogen,
3. OZG-Dashboard,
4. Direktkontakte.

3.2.1 Internet-Recherche und Fragebogen

Zunächst wurden mit einer Internet-Recherche durch die secuvera GmbH im Zeitraum von Februar bis März 2022 Hersteller und relevante Produkte identifiziert. Da zum einen die Verbreitung der einzelnen Lösungen nicht ersichtlich war, zum anderen auch einige Lösungen für den Smart-City-Markt konzipiert wurden, wurden seitens des Projektteams entsprechende Metriken definiert, um eine Eingrenzung vornehmen zu können. Beispielsweise wurden die Landeshauptstädte Deutschlands, sowie sieben weitere große Städte (basierend auf deren Einwohnerzahl) aufgrund der Annahme eines dort vorherrschenden großen OZG-Umsetzungsdrucks untersucht. Hierfür wurden Fachzeitschriften genutzt, die im Jahr 2022 mehrfach über die Umsetzung des OZGs berichtet haben [2].

Des Weiteren wurde für einen Gesamtüberblick über die großen Serviceportale der Bundesländer eine Online-Recherche nach Funktionalität, Hersteller und aktuellem Stand durchgeführt. In einigen Portalen existierten bereits einzelne Online-Anträge. Allerdings erfolgte in vielen Fällen auch ein Absprung in andere Portale, d. h. die Online-Anträge waren nicht im Portal selbst integriert, sondern lediglich über eine Schnittstelle angebunden. Da sich die Anträge je nach Kommune in ihrer Umsetzung unterschieden, blieb oftmals die Frage nach dem jeweiligen Softwarehersteller, Betreiber der Lösung oder User Interface (UI) offen.

Als weitere Metrik wurde ein Fragebogen seitens secuvera GmbH entwickelt und am 22. Februar 2022 an die OZG-Koordinatorinnen und OZG-Koordinatoren der Bundesländer sowie Ansprechpartnerinnen und Ansprechpartner der einzelnen Themenfelder zusammen mit einem erläuternden Anschreiben versendet. Diese Zielgruppe wurde anhand der Annahme ausgewählt, dass die OZG-Koordinatorinnen und OZG-

Koordinatoren sowie die Ansprechpartnerinnen und Ansprechpartner der Themenfelder über den größten Überblick der Umsetzungslandschaft der Portale auf den verschiedenen föderalen Ebenen verfügten. Die beiden Dokumente können in der Anlage nachvollzogen werden.

Bis zum Abschluss der Marktrecherche, Ende März 2022, erhielt die secuvera GmbH lediglich zwei ausgefüllte Fragebögen zurück. Aufgrund dieser wenigen Rückmeldungen und der damit einhergehenden beschränkten Vergleichbarkeit waren die Ergebnisse wenig aussagekräftig.

Grundsätzlich wurde bei der Auswertung der Fragebögen festgestellt, dass diese direkten Informationen von OZG-Koordinatorinnen und -Koordinatoren und Ansprechpartnerinnen und Ansprechpartnern sehr wertvoll waren und viele detaillierte Informationen über eine einzelne Umsetzungslösung gewonnen werden konnten. Mögliche Ursachen für die fehlenden Rückmeldungen können fehlende Ressourcen, mangelndes Interesse oder fehlendes Vertrauen in die Authentizität des Fragebogens sein. Insbesondere der letzte Punkt wurde durch vereinzelte Rückfragen hinsichtlich der Echtheit des Fragebogens über andere Kanäle deutlich. Das Projektteam bestätigte mehreren Anfragenden die Echtheit des Fragebogens, erhielt jedoch auch nach dieser Bestätigung keine weiteren Rückmeldungen mehr.

3.2.2 OZG-Dashboard

Mithilfe des OZG-Dashboards[4] wurde direkt nach Anträgen recherchiert, die bereits digital funktionsfähig sein sollten. Zum Zeitpunkt der Recherche im März 2022 waren laut OZG-Dashboard 71 Leistungen online zugänglich (Reifegrad 1 im Reifegradmodell, als PDF downloadbar) [3].

Da zum Zeitpunkt der Erhebung keine Differenzierung in unterschiedliche Reifegrade erfolgte, wurden die genannten Antragsverfahren in einem weiteren Schritt auf ihre jeweilige Reife hin untersucht. In vielen Fällen wurden hierbei Leistungen im Reifegrad 1 vorgefunden, welche lediglich als PDF downloadbar waren und nur in analoger Form eingereicht werden konnten. Da eine digitale Befüllung dieser Anträge in diesen Fällen nicht möglich war, waren solche Leistungen im Rahmen des Projektes nicht relevant.

Die Recherche über das OZG-Dashboard war für das Projekt von einem hohen Mehrwert, da über das Dashboard und die identifizierten Anträge verschiedene Informationen gewonnen werden konnten. Beispielsweise konnten im Dashboard direkt Informationen über das umsetzende Bundesland und das zuständige Ressort abgerufen werden. Sofern ein digitaler Antrag identifiziert werden konnte, wurde über das Impressum oder den HTML-Quelltext des Antrags nach den verantwortlichen Herstellern und eingesetzten Formularlösungen gesucht. Mithilfe dieser Informationen war es dem Projektteam möglich, einen Überblick darüber zu erlangen, welche Formularlösungen, Technologien und Hersteller zum damaligen Zeitpunkt am häufigsten eingesetzt wurden. Diese Informationen wurden auch im Zuge der Ansprache der Direktkontakte weiterverwendet, insbesondere, um Hersteller von Formularlösungen direkt kontaktieren zu können.

3.2.3 Direktkontakte

In den ersten Schritten der Marktanalyse stellte sich bereits heraus, dass die über die Online-Recherche und den versendeten Fragebogen gesammelten Informationen und Rückmeldungen insgesamt weniger aussagekräftig waren als erhofft. Am Markt existieren eine Vielzahl von Herstellern, die Lösungen für den E-Government-Bereich anbieten, jedoch bestehen Webportale im E-Government in der Regel nicht aus einem fertigen Produkt, das in sich abgeschlossen eingekauft oder nachgenutzt werden kann. Vielmehr existiert ein, auf die jeweiligen Aufgaben spezialisierter Verbund von Einzelkomponenten. Folglich gibt es weder einen von außen transparent einsehbaren, aktiven Markt, noch Entwickler, die vollständige Lösungen mit festen Funktionsanforderungen bewerben. Zusätzlich zeigten die Rückmeldungen zu den Fragebogen, dass es bei Fragen bezüglich Produkten wie Verwaltungsportalen, die sensible Informationen verarbeiten, ein großer Wert auf gegenseitiges Vertrauen gelegt wird, um überhaupt in einen grundlegenden Austausch zu kommen.

In diesem Kontext stellten sich die direkten persönlichen Kontakte, die vonseiten des Projektteams bereits bestanden, als wertvoll heraus. Durch vergangene Projekte und Kooperationen existierten hier

[4] https://dashboard.ozg-umsetzung.de/

Ansprechpartnerinnen und Ansprechpartner, die direkt angesprochen wurden und denen das Projekt vorgestellt werden konnte. Der große Vorteil dieser persönlichen Kontakte war es, dass hier aus der Vergangenheit bereits ein Vertrauensanker gesetzt war und teilweise auch eine Weitervermittlung an interessierte Portalbetreibende erfolgen konnte.

Durch interne Kontakte zu anderen Projekten und Arbeitsgruppen sowie die Platzierung in einschlägigen föderalen Gremien konnte durch das BSI eine erste Kontaktaufnahme zu den Teilnehmern des Städte- und Gemeindetages eines Bundeslandes erfolgen. Hierbei ist ein Kontakt zu einer großen Kommune entstanden. Ferner konnte auch ein Kontakt zu einem Landesportal hergestellt werden. Darüber sind zwei Interessensbekundungen erfolgt. Ebenfalls über einen Arbeitsgruppenkontakt wurde der Kontakt zu einer weiteren Landesbehörde hergestellt, die grundsätzliches Interesse an der Teilnahme am Projekt bekundet hatte.

Aufseiten der secuvera GmbH gab es ebenfalls Kontakte zu Behörden, Herstellern oder Dienstleistern aus vergangenen Projekten im Bereich der Sicherheitsberatung und Penetrationstests. Im Zuge der Marktrecherche wurden diese vom secuvera GmbH-Projektteam kontaktiert und zu einem Austausch eingeladen. Zu insgesamt neun Behörden und Dienstleistern existierten direkte persönliche Ansprechpartner und Ansprechpartnerinnen.

3.2.4 Auswahlkriterien

Basierend auf den Ergebnissen der Marktrecherche sollten anschließend fünf bis neun Produkte ausgewählt werden, die im Rahmen des Projekts einer IT-Sicherheitsuntersuchung unterzogen werden sollten. Hierfür wurden vorab Auswahlkriterien definiert, um einerseits einen möglichst identischen Testbereich (Scope) und damit die Vergleichbarkeit der Produkte und Testergebnisse gewährleisten zu können. Zum anderen sollte die Umsetzung der Produkte (hier: Portale) möglichst verschieden sein, um ein möglichst breites Anwendungsfeld abdecken zu können.

Da die Grundlage des Projekts durch das Onlinezugangsgesetz gebildet wurde, war das Kriterium „OZG-Bezug“ bereits bei der Marktrecherche ein grundlegendes Merkmal. Hier lag der Fokus insbesondere auf digitalisierten Antragsstrecken, die mindestens Stufe 2 im Reifegradmodell erfüllen. Demzufolge wurden nur Portale näher betrachtet, die mindestens einen Antrag anboten, der beim Ausfüllen des Formulars durch einen Formular-Assistenten unterstützt wurde. Portale, die lediglich Informationen zu den einzelnen Leistungen in Form von PDF oder Vergleichbarem anbieten konnten, wurden demzufolge nicht weiter berücksichtigt.

Da noch nicht alle Portale die gängigen Anträge, wie bspw. die Beantragung der Geburtsurkunde, auf einem einheitlichen Stand entwickelt hatten und zusätzlich für unterschiedliche föderale Ebenen unterschiedliche Leistungen existieren, wurde nicht eine spezifische Antragsstrecke für alle Portale ausgewählt. Wichtiger war die Betrachtung von spezifischen Funktionalitäten der einzelnen Antragsstrecken mit besonders großer Angriffsfläche. Ebenfalls wurde berücksichtigt, wie relevant ein Antrag für den Bürger und wie groß die Menge beispielsweise an erfassten personenbezogenen Daten war. An dieser Stelle wurden Anträge, die eine Upload-Funktion und/oder eine Benutzerauthentifizierung mittels eID integriert hatten, bevorzugt betrachtet, da diese Funktionalitäten in den meisten Portalen Einsatz fanden und so die Vergleichbarkeit der Ergebnisse besser gewährleisteten.

Um eine Vergleichbarkeit zu gewährleisten, wurden identische Antragsverfahren mit gleichem Umfang und möglichst vielen Funktionalitäten ausgewählt. Hierbei wurden, soweit möglich, unterschiedliche Formularlösungen bevorzugt berücksichtigt.

Neben den bereits genannten technischen Merkmalen spielte für die Auswahl zusätzlich auch die Kooperationsbereitschaft der Kommunen und Länder eine entscheidende Rolle.

Eine Zusammenarbeit wurde nur dann angestoßen, sofern das Projekt auf Interesse bei Kommunen und Ländern gestoßen ist und eine Zustimmung zur Teilnahme am Projekt erfolgte. Hierzu wurden bei Interessensbekundung Vorgespräche geführt.

3.2.5 Auswahl der Portale

Anhand der in Kapitel 3.2.4 aufgeführten Auswahlkriterien sollten Portale ausgewählt werden, die ein möglichst breites Anwendungsfeld abdecken. Insgesamt konnten so fünf Portale für einen anschließenden Penetrationstest ausgewählt werden, bei denen sowohl die projekt- und fachspezifischen Kriterien als auch die organisatorischen Rahmenbedingungen erfüllt werden konnten. Im Rahmen dieses Projekts wurden folgende Portale betrachtet:

Nummer und Art des Portals	***Antragsstrecke***	***Upload-Funktion***	***Verwendung eID***	***Formularlösung***
Portal A Serviceportal eines Landes	Test Antragsstrecke	Ja	Ja	White-Label-Lösung 1 + White-Label-Lösung 2
Portal B Kommunalportal eines Landes	Einfache Meldebescheinigung	Nein	Ja	White-Label-Lösung 1
Portal C Portal einer Kommune	Test-Antragsstrecke	Ja	Nein	White-Label-Lösung 3 + Eigenentwicklung
Portal D Serviceportal eines Landes	Halteverbot für Umzugstransport	Ja	Nein	Eigenentwicklung einer Kommune
Portal E Portal einer Kommune	Führerschein, Karteikarten-abschrift + Geobasisdaten online beantragen	Ja	Ja	White-Label-Lösung 3

Tabelle 2: Auswahl der Portale

4 Angriffs- und Durchführungskatalog

Ziel des Projekts MaSiGov war es, unter anderem Kompetenzen im Hinblick auf die IT-Sicherheit der OZG-Umsetzungen durch die Durchführung von Schwachstellenanalysen zu erlangen. Um eine Methodik für die Durchführung von Schwachstellenanalysen zu entwickeln, wurde ein „Angriffs- und Durchführungskatalog“ erstellt. Ziel dieser Kataloge war es, eine gleichbleibende Güte der Tests und eine hohe Qualität sowie Vergleichbarkeit der einzelnen Prüfungen zu gewährleisten. Der Angriffskatalog beinhaltete eine Auflistung aller im Rahmen der Prüfung möglichen Angriffe auf die ausgewählten Testgegenstände. Für jedes Portal wurde zusätzlich zum Angriffskatalog ein speziell auf die Besonderheiten angepasster Durchführungskatalog erstellt, in dem für das jeweilige Portal konkret ausgewählt wurde, welche Prüfungen angewandt werden. Durch die Bearbeitung der einzelnen Durchführungskataloge während der Prüfungen wurde stets ein Negativ-Reporting erstellt. Bei einem solchen Reporting werden alle Ergebnisse der durchgeführten Tests angegeben, auch wenn sie aus Sicht der Anwendung zu keiner Schwachstelle oder zu keinem Fehler führen.

4.1 Risiko-Identifikation und Risiko-Analyse

Um mögliche Angriffe auf E-Government-Lösungen erfassen zu können, wurde zunächst eine Risiko-Identifikation und im Anschluss eine Risiko-Analyse durchgeführt. Auf Basis der Risiko-Analyse wurden mögliche Angriffe (Testszenarien) für den Angriffskatalog abgeleitet. Die Ableitung der Angriffe auf Basis der Risiko-Analyse erfolgte zunächst losgelöst von gängigen Test-Standards, die bereits am Markt existierten. Nach Abschluss der Definition der einzelnen Testszenarien wurden diese gängigen Test-Standards gegenübergestellt, um eine möglichst lückenlose Teststrategie aufzustellen.

Als Basis für den Angriffskatalog wurde im Anschluss der Web Security Testing Guide der OWASP [4] in Version 4.2 gewählt. Es handelt sich hierbei um einen weit verbreiteten Standard, der sehr ausführlich die Vorgehensweise für die Identifizierung von Schwachstellen in Webapplikationen beschreibt. Im Rahmen der Definition des Angriffskatalogs wurde festgestellt, dass fast alle identifizierten Bedrohungen und abgeleitete Tests auch auf Prüfungen des OWASP Testing Guides abgebildet werden konnten. Es existiert ein weiteres Dokument der OWASP, der Application Security Verification Standard (ASVS) [5] in Version 4.0.3. Dieses Dokument beinhaltet einen Testkatalog, der an Architekten, Entwickler, Sicherheitsexperten, Tool-Hersteller und Verbraucher gerichtet ist, um Informationssicherheit in Anwendungen zu implementieren und zu verifizieren.

Der Testing Guide berücksichtigt einige im OZG-Kontext wichtige Punkte, wie beispielsweise Multi-Faktor-Authentifizierung, nicht ausführlich. Aus diesem Grund wurden die beiden Standards miteinander kombiniert, um noch fehlende Punkte und alle für das Projekt relevanten Prüfungen in den Angriffskatalog aufzunehmen.

4.2 Angriffskatalog

Der erstellte Angriffskatalog beinhaltete in Summe 135 Einzelprüfungen, die pro Portal ausgeführt werden können. Ein Teil der Prüfungen fokussierte sich auf die Prüfung der Infrastruktur und der Transportverschlüsselung, während sich der Großteil der Prüfungen auf die Anwendung selbst bezog.

Die Prüfungen starteten hierbei mit einem „Information Gathering“, also einer Informationsgewinnung, und gingen darüber hinaus auf eine Vielzahl von weiteren Kategorien ein, wie beispielsweise: Prüfung der Authentifizierung und Authentisierung, Prüfung der Business Logic und Input Validation. Schwachstellen im Kontext der Business Logic bezogen sich auf Verwundbarkeiten im Design und in der Implementierung einer Anwendung, die zu einem unerwünschten Verhalten der Anwendung führen können. Werden Schwachstellen im Bereich der Input-Validierung identifiziert, sind diese darauf zurückzuführen, dass Eingaben der Benutzer von der Anwendung nicht korrekt überprüft werden und ein Angreifer so gegebenenfalls in der Lage ist, schadhaften Inhalt in die Anwendung einzuschleusen.

Die Prüfungen der Anwendung verfolgten hierbei zwei Prüfziele. Zum einen lagen technische Schwachstellen im Fokus der Prüfungen. Hierunter fallen beispielsweise Schwachstellen, die auf eine fehlerhafte Prüfung der Benutzereingaben zurückzuführen sind. Weiterhin erfolgte eine Prüfung des Berechtigungsmodells. In diesem Schritt wurde geprüft, ob eine horizontale oder vertikale Rechteausweitung möglich ist. Eine horizontale Rechteausweitung liegt beispielsweise dann vor, wenn Kunden unberechtigt auf Daten anderer Kunden zugreifen können. Eine vertikale Rechteausweitung liegt dann vor, wenn beispielsweise ein Kunde Funktionen aufruft oder Daten einsehen kann, die eigentlich einem Administrator vorbehalten sind.

4.3 Durchführungskatalog

Nach Fertigstellung und Abnahme des Angriffskatalogs wurden gemeinsam mit den Ansprechpartnern der zu prüfenden Portale Scoping-Termine durchgeführt. Im Rahmen dieser Besprechungen wurde durch die Ansprechpartner und Ansprechpartnerinnen das jeweilige Portal vorgestellt, der genaue Scope der Prüfungen festgelegt und ein Leistungsschein erstellt. Auf Basis der übergebenen Informationen wurde durch die Prüfer und Prüferinnen der secuvera GmbH für jedes Portal ein individueller Durchführungskatalog erstellt, der alle ausgewählten Tests des Angriffskatalogs listet und im Nachgang der Prüfung an die Ansprechpartner übergeben wurde. Bereits vor Beginn der Prüfungen wurde der Katalog erstellt und vorausgefüllt. Dies bedeutet, dass in einigen Fällen bereits im Vorfeld bekannt war, welche Technologien im Einsatz sind oder welche Funktionalitäten von den Portalen nicht angeboten wurden. Diese Prüfungen konnten daher bereits vor Testbeginn aus dem Scope genommen und die Prüfungszeit für andere Prüfungen aufgewendet werden.

Während der Prüfung wurde der Durchführungskatalog durch die Prüfer vollständig ausgefüllt. Folgende Notationen waren hierbei für die einzelnen Prüfungen zulässig:

Notation	***Bedeutung***	***Erklärung***
K	Kein Befund	Der Test wurde im Rahmen der Schwachstellenanalyse durchgeführt und führte zu keiner Schwachstelle oder Sicherheitshinweis.
N	Nicht prüfbar	Die Funktion war nicht vorhanden oder nicht prüfbar, da nicht funktional. Falls die Funktionen vorhanden, aber nicht prüfbar waren, wird in der Kommentarspalte des Durchführungskatalogs ein Kommentar zu den Gründen hinterlegt.
S_xx/W_xx	Schwachstelle	Der Test wurde durchgeführt und es konnte eine Schwachstelle identifiziert werden. Hierbei wurde zwischen Systemprüfungen (S) und Webanwendungsprüfungen (W) unterschieden.
H_xx	Sicherheitshinweis	Der Test wurde durchgeführt und es konnte ein Sicherheitshinweis identifiziert werden. Ein Sicherheitshinweis kann ein begünstigender Faktor für eine Schwachstelle darstellen.
O	Nicht im Fokus / Out of Scope	Dieser Test wurde nicht durchgeführt, da die Funktionalität nicht im Fokus der Prüfung stand. Wurden bestimmte Funktionen explizit aus der Prüfung ausgeschlossen, wurden diese im Rahmen der Penetrationstests nicht überprüft.

Tabelle 3: Notationen

Durch die Abarbeitung des Durchführungskatalogs konnte stets nachvollzogen werden, welche Tests mit welchem Ergebnis durchgeführt wurden. Dabei wurde ebenfalls ein Negativ-Reporting erstellt. Bei einem

solchen Reporting wurden alle Ergebnisse der durchgeführten Tests angegeben, auch wenn sie aus Sicht der Anwendung zu keiner Schwachstelle oder zu einem Fehler führten.

5 Durchführung der Schwachstellenanalysen

Für jedes ausgewählte Produkt wurde eine Schwachstellenanalyse auf Basis des erstellten Durchführungskatalogs vorgenommen. Der Ablauf der einzelnen Schwachstellenanalysen wird in den folgenden Kapiteln beschrieben.

5.1 Vorgehensweise analog zum Durchführungskonzept Penetrationstests

Um eine effektive und nachvollziehbare Durchführung mit kalkulierbarem Risiko sicherzustellen, wurde die Vorgehensweise der Prüfung an das „Durchführungskonzept Penetrationstests des BSI“ angelehnt [6]. Anhand der in diesem Dokument beschriebenen Kriterien wurden die durchgeführten Penetrationstests klassifiziert und das Scoping auf dessen Basis durchgeführt. Die in der folgenden Darstellung farblich dunkel hervorgehobenen Kriterien wurden für die Durchführung ausgewählt.

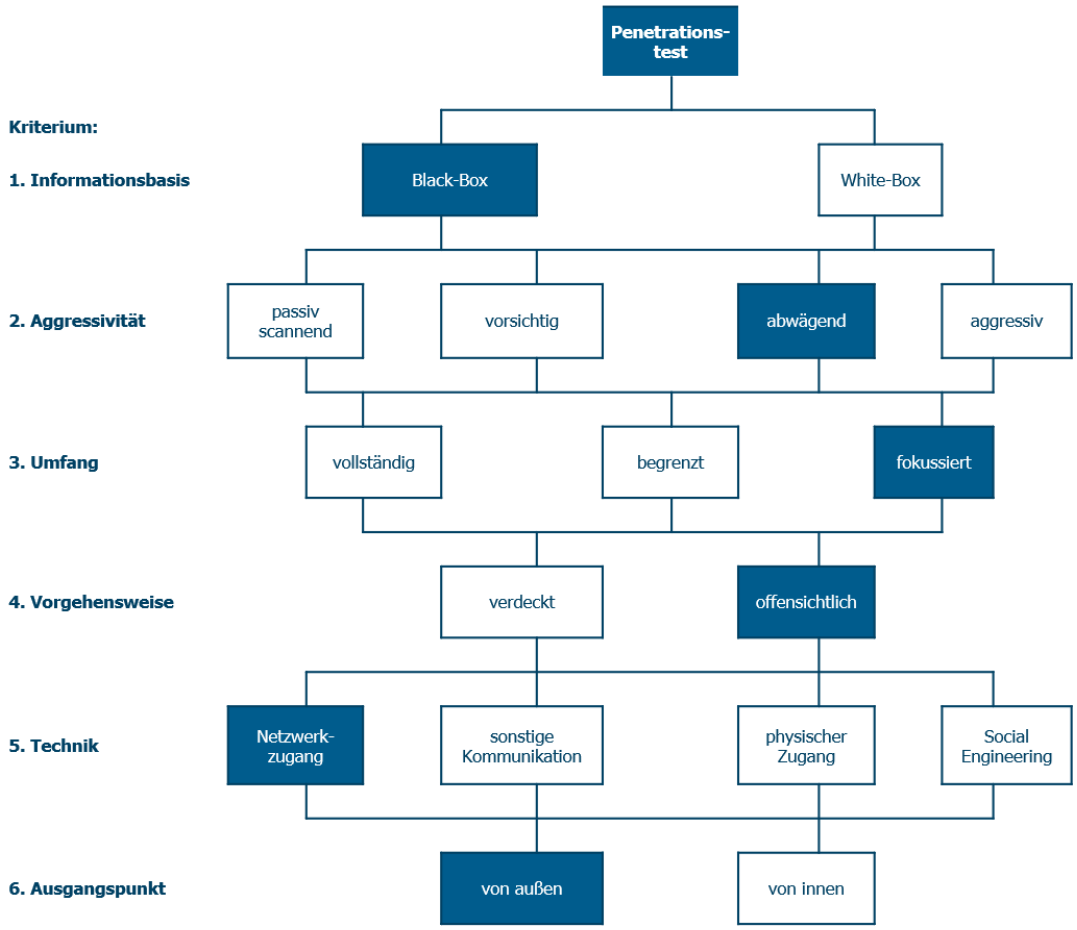

Abbildung 2: Vorgehensweise nach Durchführungskonzept Penetrationstest des BSI

Das Kriterium „Informationsbasis“ beschreibt die Wissensbasis der Penetrationstester für die Durchführung der Prüfung. Hierbei wurde ein Black-Box-Ansatz gewählt. Den Testern wurden bestimmte Informationen zur Verfügung gestellt, jedoch erfolgte die Prüfung hauptsächlich aus der Sicht eines Angreifers, d. h. über das Internet und ohne Insider-Wissen.

Für das Kriterium der „Aggressivität“ wurde die Stufe „abwägend“ gewählt. Um Schwachstellen nachweisen zu können, wurden einzelne Schwachstellen ausgenutzt. Es erfolgten jedoch keine destruktiven Angriffe wie beispielsweise Denial-of-Service-Angriffe. Insgesamt wurde bei einer möglichen Ausnutzung sehr stark abgewogen, inwiefern Konsequenzen zu erwarten sind und inwiefern eine Ausnutzung notwendig ist, um eine Schwachstelle sicher nachzuweisen.

Der „Umfang“ der einzelnen Schwachstellenanalysen erfolgte aufgrund des vorgegebenen Projektrahmens sehr fokussiert. Die Portale, die im Fokus der Prüfungen standen, stellten komplexe Anwendungen dar, die in der Regel eine Vielzahl an Funktionen anbieten. Für die Tests wurde je Prüfgegenstand versucht, einen individuellen Scope zu finden, in dem sicherheitstechnisch möglichst interessante Komponenten der Anwendungen abgebildet sind. In der Regel wurden daher Antragsstrecken mit möglichst vielen Funktionen, beispielsweise mit Upload-Funktionen, überprüft.

Die „Vorgehensweise“ war „offensichtlich“, da den Ansprechpartnern der jeweiligen Portale die durchzuführende Schwachstellenanalyse bekannt war. Das Testteam versuchte daher nicht, die Aktivitäten zu verschleiern.

Die Prüfungen erfolgten über einen „Netzwerkzugang“ (Kriterium: „Technik“) und „von außen“ (Kriterium: „Ausgangspunkt“), analog zu einem echten Angriff über das Internet.

5.2 Ablauf der Schwachstellenanalysen

Jede durchgeführte Schwachstellenanalyse wurde im Rahmen des Projekts als ein einzelnes Teilprojekt betrachtet. Die fünf ausgewählten Teilprojekte wurden hierzu in verschiedene Phasen eingeteilt. Das folgende Schaubild beschreibt die einzelnen Phasen mit den durchzuführenden Punkten:

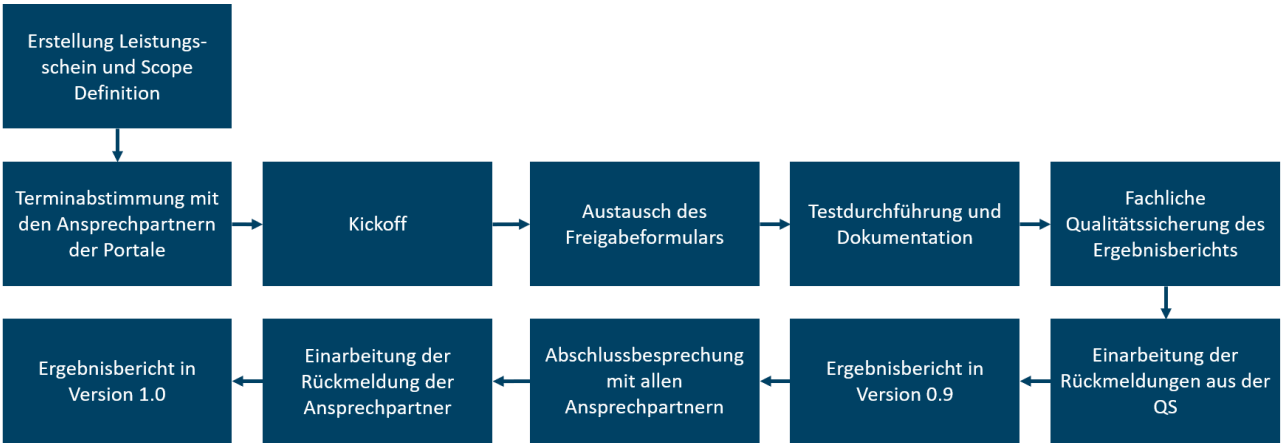

Abbildung 3: Ablauf der Schwachstellenanalysen

Die Abbildung zeigt, dass jede Schwachstelle mit der Erstellung eines Leistungsscheins und einer Definition des Scopes startete. Im Anschluss, oder bereits während der initialen Besprechung, erfolgte die Terminabstimmung zwischen allen Beteiligten. Vor Testbeginn wurde noch eine Kickoff-Besprechung durchgeführt sowie das Freigabeformular ausgetauscht. Im Anschluss folgte die eigentliche Durchführung der Schwachstellenanalyse sowie die Dokumentationsphase. Der erstellte Ergebnisbericht wurde durch einen zweiten Penetrationstester einer fachlichen Qualitätssicherung unterzogen. Zusätzlich erfolgte eine Qualitätssicherung durch das BSI sowie ein Lektorat. Die Ansprechpartner der Service- und Kommunalportale erhielten anschließend eine Berichtsversion 0.9, über die gemeinsam in der Abschlussbesprechung gesprochen wurde. Ergab sich aus diesem Termin noch Änderungsbedarf am Ergebnisbericht, wurden diese Änderungen in die Version 1.0 des Berichts eingearbeitet.

5.2.1 Erstellung Leistungsschein und Scope-Definition

Im Verlauf der einzelnen Teilprojekte erfolgte im Rahmen der Vorbereitungsphase zunächst ein Kennenlerntermin mit den einzelnen Produktverantwortlichen. Während dieser Termine wurde durch das BSI zuerst das Projekt MaSiGov vorgestellt. Weiterhin erfolgte eine Einführung in die grundsätzliche

Vorgehensweise von Schwachstellenanalysen durch die secuvera GmbH. Die Ansprechpartner erhielten die Gelegenheit, die Anwendungen, also die späteren Testgegenstände, vorzustellen.

Im Verlauf der einzelnen Gespräche stellte sich in den meisten Fällen heraus, dass im Rahmen der Entwicklung und des Betriebs der einzelnen Portale viele Parteien involviert sind und die Planung einer Schwachstellenanalyse bzw. die Festlegung eines Scopes eine große Herausforderung sind. In der Regel erfolgten daher mehrere Scoping-Termine mit den entsprechenden Ansprechpartnern aufseiten der Betreiber.

Im Rahmen dieser Termine wurde gemeinsam mit den Ansprechpartnern identifiziert, welche Bestandteile der Portale im Rahmen einer Schwachstellenanalyse geprüft werden sollten, um einen aussagekräftigen Test zu erhalten. Hierbei kamen die folgenden Punkte in der Regel zum Tragen:

- Die Software zum Betrieb der unterschiedlichen Portale wird in regelmäßigen Abständen aktualisiert und erhält regelmäßig neue Funktionalitäten oder wird in der Optik angepasst. Daher wurde in einigen Fällen das Portal selbst sowie insbesondere Komponenten zum „Suchen & Finden“ oder „Zuständigkeitsfinder“ in den Test einbezogen.
- Über die Portale können Bürger Anträge abgeben und ggf. auch verwalten. Diese Antragsstrecken bieten auch für Angreifer die Möglichkeit, mit der Anwendung zu interagieren und Angriffe zu platzieren. Daher wurden für die Prüfungen in allen Fällen auch Antragsstrecken ausgewählt, über die die Anwendung angegriffen werden könnte. Wenn vorhanden, wurden hierbei Antragsstrecken, die komplexere Funktionalitäten wie beispielsweise eine Upload-Funktion anboten, ausgewählt. Verwendete ein Serviceportal mehrere Formulartechnologien, wurden nach Möglichkeit mehrere Antragsstrecken auf Basis der verschiedenen Technologien ausgewählt.

Im Anschluss erhielten die Betreiber der Portale einen Leistungsschein, der die durchzuführende Prüfung, also den Scope der Prüfung, beschreibt und die Vorgehensweise, die angesetzt werden sollte, festhält.

5.2.2 Terminabstimmung und Kickoff

Bereits in den initialen Besprechungen stellte sich heraus, dass viele Ansprechpartner in die Durchführung solcher Schwachstellenanalysen einzubinden waren. Eine Terminabstimmung und die Festlegung eines Testzeitraums stellten daher in einigen Fällen eine Herausforderung dar. Seitens der Entwickler gab es in allen Fällen bereits einschlägige Erfahrungen mit Schwachstellenanalysen des jeweiligen Produkts.

Alle Testgegenstände, die für die Prüfungen ausgewählt wurden, konnten in einer Testumgebung geprüft und analysiert werden. Da die Testumgebungen jedoch auch für eigene Tests der Betreiber verwendet werden und zudem die Softwarestände eher selten stabil sind, war die Testkoordination und -planung sehr aufwändig.

In allen Fällen konnte jedoch eine Terminabstimmung erfolgreich durchgeführt und ein gemeinsamer Projektplan erstellt werden. In der Regel wurde durch die Tester ein Testzeitraum von zwei Wochen angesetzt, in dem der Durchführungskatalog geprüft werden konnte.

Vor Testbeginn erfolgte in der Regel noch eine kurze Abstimmung, um letzte Fragen zu besprechen.

5.2.3 Testdurchführung, fachliche Qualitätssicherung und Lektorat

Die Prüfungen erfolgten zunächst vor allem automatisiert mithilfe von Burp Suite Professional[5]. Je nach Szenario wurden weitere Werkzeuge in die Tests einbezogen, um die automatisiert prüfbaren Tests des Durchführungskatalogs zu prüfen. Hierfür wurden Tools wie nmap[6], OpenVAS[7], testssl[8] oder sqlmap[9] verwendet. Vor jeder durchgeführten Prüfung wurden die eingesetzten Tools auf die jeweils aktuellste

5 https://portswigger.net/burp/pro
6 https://nmap.org/
7 https://www.openvas.org/index-de.html
8 https://testssl.sh/
9 https://sqlmap.org/

Version aktualisiert. Die Ergebnisse wurden im Nachgang manuell verifiziert und bewertet. Nach Abschluss der automatisierten Tests wurden die Bestandteile des Durchführungskatalogs geprüft, die ausschließlich manuell prüfbar sind. Der jeweilige Tester erstellte dann pro durchgeführter Prüfung einen ausführlichen Ergebnisbericht, in dem alle gefundenen Schwachstellen beschrieben sind sowie die entsprechende Testvorgehensweise festgehalten ist.

Im Anschluss an die Prüfungen übergab der entsprechende Tester den Bericht und alle Ergebnisse an einen zweiten Tester der secuvera GmbH, der eine unabhängige fachliche Qualitätssicherung durchführte. Ziel dieser Qualitätssicherung war es, Fehler in den Tests nachzuweisen, die Einhaltung der Durchführungskataloge sicherzustellen und alle Ergebnisse nochmals auf Vollständigkeit und Korrektheit zu kontrollieren. Nach Abschluss dieser Qualitätssicherung erfolgte eine weitere qualitätssichernde Maßnahme durch das BSI.

Ein Lektorat wurde ebenfalls durchgeführt, um die sprachliche Qualität des Ergebnisberichts zu sichern.

5.2.4 Abschlussbesprechungen

Nach Fertigstellung des Ergebnisberichts in der Version 0.9 erhielten die Ansprechpartner dieses Dokument.

Gemeinsam wurde dann eine Abschlussbesprechung terminiert, in deren Rahmen die Ergebnisse den jeweiligen Ansprechpartnern vorgestellt wurden. Die Ansprechpartner erhielten hier Gelegenheit, alle offenen Fragen zu stellen oder zu gewissen Funden Stellung zu beziehen. Beispielsweise war es bei einigen Portalen der Fall, dass Schwachstellen in den Upload-Funktionen der Anwendungen identifiziert werden konnten, da keine Virenscanner aktiviert waren. Dabei stellte sich heraus, dass bei einigen der Portale auf dem Testsystem kein Virenscanner aktiv war, auf dem Produktivsystem jedoch Sicherheitsmechanismen aktiv waren, die den Upload von Schadcode verhindern würden.

5.2.5 Nachtest

Wurden Schwachstellen im Rahmen der Analysen identifiziert, erhielten die Ansprechpartner das Angebot, die Behebung dieser Schwachstellen durch einen selektiven Nachtest verifizieren zu lassen.

Im Rahmen des Projekts wurde kein Nachtest in Anspruch genommen. Die gefundenen Schwachstellen wurden durch die Verantwortlichen der geprüften Portale aufgenommen. Die Verantwortlichen gaben an, die Behebung in nachfolgenden, selbst beauftragten Schwachstellenanalysen prüfen zu wollen.

5.3 Kategorisierung der Ergebnisse

Funde, die im Laufe der Prüfungen identifiziert wurden, wurden in zwei Kategorien eingeteilt. Bei der ersten Kategorie handelt es sich um Schwachstellen, die aus Sicht der Prüfer ausnutzbar sind und einen direkten Einfluss auf die Sicherheit der Anwendung haben: In der Regel bringt die Ausnutzung einer solchen Schwachstelle einen Vertraulichkeits- oder Integritätsverlust mit sich oder führt zu einer Einschränkung der Verfügbarkeit des Diensts oder des kompletten Systems.

Bei der zweiten Kategorie handelt es sich um sogenannte Sicherheitshinweise. Während der Prüfung werden Sicherheitsprobleme identifiziert, die nicht klar als Schwachstelle zu bewerten sind, etwa weil von ihnen kein direktes Risiko ausgeht oder es sich nur um Abweichungen von gängigen Sicherheitsstandards bzw. Best-Practices handelt, diese jedoch keinen direkten ausnutzbaren Angriff zur Folge haben. Diese werden als Hinweis eingestuft und werden bei der Ermittlung des Sicherheitsniveaus nicht beachtet.

5.4 Schwachstellenbewertung

Zur Ermittlung des Risikograds von Schwachstellen wird das Common Vulnerability Scoring System (CVSS) in Version 3.1[10] verwendet. CVSS ist der Industriestandard zur Bewertung von Schwachstellen und wurde von der Organisation FIRST (Forum of Incident Response and Security Teams) entwickelt.

Für jede gefundene Schwachstelle im Rahmen des Projekts wurde der CVSS Base Score berechnet und als Kritikalitätsbewertung der Schwachstelle in den Bericht aufgenommen. Der Base Score setzt sich zusammen aus den Voraussetzungen, die für einen erfolgreichen Angriff gegeben sein müssen (Exploitability Metrics), und den Konsequenzen, die die Ausnutzung der Schwachstelle mit sich bringt (Impact Metrics). Für die Voraussetzungen sind die folgenden Werte relevant:

- **Attack Vector**: In dieser Variable wird reflektiert, wie die Ausnutzung der Schwachstelle erfolgt. Beispielsweise wird hier unterschieden, ob eine Ausnutzung über ein Netzwerk oder lokal an der entsprechenden Komponente erfolgen muss.
- **Attack Complexity**: In den Werten „low“ oder „high“ wird die Komplexität des Angriffs bewertet. Ein Angriff, der wiederholbaren Erfolg verspricht, ohne dass besonderes Equipment oder Know-how vorliegen muss, wird als niedrig komplex eingestuft, während ein Angriff, der von Randbedingungen abhängt oder darauf begründet ist, dass sich ein Angreifer zunächst in die Umgebung einarbeiten muss, als „high“ eingestuft wird.
- **Privileges Required**: In dieser Variable wird reflektiert, ob der Angriff als anonymer Angreifer durchgeführt werden kann oder der Angreifer bestimmte Berechtigungen am entsprechenden Dienst besitzen muss.
- **User Interaction**: In einigen Fällen können Schwachstellen nur ausgenutzt werden, indem Nutzer eine bestimmte Interaktion mit dem verwundbaren Dienst durchführen, beispielsweise einen Klick auf einen Link. Sollte dies der Fall sein, wird in dieser Kategorie der Wert „required“ gesetzt.

Die Auswirkungen der Schwachstelle werden in den folgenden Variablen bewertet:

- **Confidentiality Impact**: Ist dieser Wert gesetzt, bedeutet dies, dass die Ausnutzung der Schwachstelle zu einem Vertraulichkeitsverlust führt. Je nach Schwere kann hier eine Einstufung in die Werte „high“ oder „low“ erfolgen.
- **Integrity Impact**: Ist dieser Wert gesetzt, bedeutet dies, dass die Ausnutzung der Schwachstelle zu einem Integritätsverlust führt. Je nach Schwere kann hier eine Einstufung in die Werte „high“ oder „low“ erfolgen.
- **Availability Impact**: Dieser Wert beschreibt eine Auswirkung der Ausnutzung der Schwachstelle auf die Verfügbarkeit. Analog zu den beiden obigen Variablen kann eine Einstufung in die Kategorien

[10] https://www.first.org/cvss/calculator/3.1

„low“ oder „high“ erfolgen, sofern die Verfügbarkeit des Diensts oder des gesamten Systems beeinträchtigt ist.

Zusätzlich existiert die Variable „Scope“. Hierbei kann der Wert „unchanged“ gewählt werden, wenn die verwundbare Komponente auch die Komponente ist, auf die eine Schwachstellenausnutzung Auswirkung hat. Der Wert „changed“ wird gewählt, wenn eine verwundbare Komponente existiert, die Ausnutzung der Schwachstelle aber Auswirkungen auf andere Komponenten hat.

Jede Schwachstelle wird anhand der skizzierten Metriken bewertet, sodass auf Basis einer von FIRST definierten Formel der Base Score auf einer Skala von null bis zehn entsteht. In der folgenden Tabelle wird der ermittelte Wert einem Risikograd zugewiesen.

Risikograd	***Base-Score***
Geringer Risikograd	0.1 – 3.9
Mittlerer Risikograd	4.0 – 6.9
Hoher Risikograd	7.0 – 8.9
Kritischer Risikograd	9.0 – 10.0

Tabelle 4: Zuordnung Risikograd zu Base Score

6 Erkenntnisse und Statistik

Es wurden insgesamt fünf Schwachstellenanalysen durchgeführt. Wie in den vorherigen Kapiteln skizziert, lag der Fokus zum einen auf Schwachstellen in der Infrastruktur (Systemebene), zum anderen auf Schwachstellen, die in der getesteten Anwendung (Anwendungsebene) vorhanden waren.

Die Prüfungen entlang des erstellten Durchführungskatalogs erfolgten zunächst mittels automatisierter Scanwerkzeuge. Im Anschluss daran wurden die Werkzeugergebnisse manuell verifiziert, um sog. False Positives möglichst ausschließen zu können. Die Tests wurden stets durch manuelle Methoden ergänzt, um im Prinzip bedingte Schwächen der toolgestützten Tests auszugleichen.

In jedem der geprüften Testgegenstände konnten im Rahmen der Prüfungen Schwachstellen gefunden werden. Erfreulicherweise konnten in keinem Fall Schwachstellen mit hohem oder kritischem Risikograd identifiziert werden. Alle erkannten Schwachstellen bewegten sich maximal im Bereich eines mittleren Risikograds. Dennoch konnten bestimmte Funde wiederholt identifiziert werden, sodass diese im Folgenden aufgegriffen werden.

6.1 Schwachstellen auf Systemebene

Im Rahmen der Prüfungen wurden fünf Systeme auf Schwachstellen untersucht. Auf allen geprüften Systemen konnten Schwachstellen mit mittlerem Risikograd identifiziert werden, sodass jeweils ein mittleres Sicherheitsniveau attestiert wurde. Die folgende Tabelle zeigt tabellarisch die identifizierten systembasierten Schwachstellen je Portal.

	Denial-of-Service durch TLS-Einstellungen (D(HE)ater-Angriff)	**Secure Client-Initiated Renegotiation möglich**
Portal A	X	-
Portal B	X	-
Portal C	X	-
Portal D	X	-
Portal E	-	X

Tabelle 5: Darstellung systembasierter Schwachstellen je Portal

Während der Prüfungen wurden die Systeme zunächst im Rahmen eines Portscans auf allen 65.535 Ports TCP und auf den „Common Ports“ UDP auf erreichbare Dienste untersucht. Im Anschluss erfolgte eine Analyse der erreichbaren Dienste und eine Suche nach Schwachstellen. Bereits nach Abschluss der Portscans wurde deutlich, dass die untersuchten Systeme ausschließlich für die Bereitstellung der Portaldienste verwendet werden. Diese Erkenntnis ist positiv hervorzuheben, da keines der geprüften Systeme weitere Dienste anbot, die einem Angreifer zusätzliche Angriffsfläche für einen Angriff bieten würden.

Alle Schwachstellen, die im weiteren Verlauf der Prüfung identifiziert werden konnten, beziehen sich auf die vom Server eingesetzte TLS-Konfiguration. Im Rahmen der Prüfung der Transportverschlüsselung wurde ein Abgleich der vorherrschenden Konfiguration, bezogen auf die Konfiguration und die eingesetzten Cipher Suites, mit den Empfehlungen der Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI-TR-02102-2 sowie TR-03116-4) vorgenommen [7] [8].

In den beiden genannten Richtlinien wird empfohlen, nur die Verschlüsselungsprotokolle TLS 1.2 bzw. TLS 1.3 und die darin als sicher geltenden Cipher Suites zu nutzen. Ein weiteres positiv hervorzuhebendes Resultat der Prüfungen war, dass alle getesteten Webserver ausschließlich verschlüsselt kommunizieren und keine veralteten TLS-Protokollversionen eingesetzt werden. Alle getesteten Webserver boten ausschließlich die Protokollversionen TLS 1.2 und TLS 1.3 an.

Dennoch konnten Probleme mit der TLS-Konfiguration identifiziert werden, die als Schwachstelle bewertet wurden.

Bei vier von fünf getesteten Systemen bot der Server Cipher Suites an, die den Schlüsselaustausch „Diffie-Hellman Ephemeral“ (kurz „DHE“) verwenden. Die Verwendung des DHE-Schlüsselaustauschs kann möglicherweise für Denial-of-Service-Angriffe missbraucht werden, indem Angreifer den Schlüsselaustausch bewusst falsch durchführen, was zur Folge hat, dass der Server unentwegt neue Schlüssel berechnet. Da die Schlüsselberechnung viel Rechenleistung beansprucht, ist es hierüber gegebenenfalls möglich, den Server auszulasten und seine Erreichbarkeit damit negativ zu beeinflussen. Dieser Angriff ist als „D(He)ater“ bekannt. Die Verwendung der im Hinweis genannten Cipher Suites sollte deaktiviert werden, sodass nur noch Cipher Suites mit dem ECDHE-Schlüsselaustausch (EC = „Elliptic Curve“) angeboten werden. Dieser Schlüsselaustausch ist zum aktuellen Zeitpunkt nicht verwundbar, da hier deutlich kürzere Schlüssellängen verwendet werden können als bei einem DHE-Schlüsselaustausch ohne elliptische Kurven. Durch die Verwendung von kürzeren Schlüssellängen beim ECDHE-Schlüsselaustausch verringert sich die benötigte Rechenleistung, was die Auswirkungen des Angriffs stark einschränkt. Diese Schwachstelle wurde mit mittlerem Risikograd gewertet.

Weiterhin wurde in einem Fall Secure Client-Initiated Renegotiation durch das System angeboten. Bei einer TLS-Renegotiation werden bestehende TLS-Verbindungsparameter neu ausgehandelt. Im Falle von Secure Renegotiation sind dabei serverseitig deutlich mehr Ressourcen als beim Client notwendig. Ist es dem Client in der Verbindung erlaubt, diese Secure Renegotiation selbst anzustoßen, so kann dies für einen Denial-of-Service-Angriff ausgenutzt werden. Secure Renegotiation sollte nur vom Server und nicht vom Client initiierbar sein. Wenn möglich, sollte TLS-Renegotiation allgemein deaktiviert werden. Diese Schwachstelle wurde ebenfalls mit mittlerem Risikograd gewertet.

Neben diesen Schwachstellen wurden auch zwei Sicherheitshinweise identifiziert, die gehäuft auftraten.

Ein Abgleich mit den genannten Technischen Richtlinien verdeutlichte, dass zwar lediglich die Protokollversionen TLS 1.2 und TLS 1.3 im Einsatz sind, jedoch in vier von fünf Schwachstellenanalysen eine Vielzahl von Cipher Suites verwendet werden, die nicht von der genannten TR empfohlen werden. Lediglich ein geprüftes Portal bot eine zu den TR konforme Konfiguration der Cipher Suites an. Grundsätzlich wird hier eine Anpassung der TLS-Konfiguration empfohlen, sodass durch den Webserver nur die in den Richtlinien empfohlenen Protokolle und Cipher Suites angeboten werden.

Bei drei von fünf Portalen konnten Auffälligkeiten in der Konfiguration der verwendeten TLS-Zertifikate identifiziert werden. Die Auffälligkeiten bezogen sich auf Abweichungen von Best-Practices und wurden daher als Sicherheitshinweis bewertet. Es konnte in keinem Fall ein direkter Angriff abgeleitet werden.

6.2 Schwachstellen auf Anwendungsebene

Ein Portal, das im Rahmen der Schwachstellenanalyse untersucht wurde, wies Schwachstellen mit niedrigem Risikograd auf. Diesem Portal konnte in der Folge ein hohes Sicherheitsniveau attestiert werden. Hierbei ist anzumerken, dass bei diesem Portal keine Upload-Funktion im Prüfungs-Scope war.

Die weiteren vier Portale, die untersucht wurden, besaßen alle eine Upload-Funktion, über die Bürgerinnen und Bürger Dokumente hochladen können, die für die Antragsstellung notwendig sind. Alle vier dieser Portale wiesen Schwachstellen mit mittlerem Risikograd im Kontext der Upload-Funktion auf. Diesen Portalen wurde jeweils ein mittleres Sicherheitsniveau attestiert. Die folgende Tabelle zeigt die identifizierten Schwachstellen je geprüftes Portal. In den folgenden Unterkapiteln werden die identifizierten Schwachstellen zusammengefasst und erläutert.

Kurzbeschreibung Schwachstelle	Portal A	Portal B	Portal C	Portal D	Portal E
Verwundbare Software im Einsatz (siehe Kapitel 6.2.1)	X	X	X	-	-
Verwundbare Upload-Funktion (siehe Kapitel 6.2.2)	X	-	X	X	X
Potentieller DoS (siehe Kapitel 6.2.3)	-	-	-	X	-
Mögliche Übertragung von sensiblen Informationen (siehe Kapitel 6.2.5)	-	X	X	-	X
Unsichere Weiterleitung (siehe Kapitel 6.2.4)	X	-	-	-	-
Secure-Merkmal im Cookie fehlt (siehe Kapitel 6.2.6)	-	-	X	-	-

Tabelle 6: Darstellung anwendungsbasierter Schwachstellen je Portal

6.2.1 Schwachstellen im Kontext eingesetzter Software

Im Zuge einer Schwachstellenanalyse wurde festgestellt, dass ein Webserver in einer Version betrieben wird, die ausnutzbare Schwachstellen besitzt. Im konkreten Fall waren für die eingesetzte Version Schwachstellen öffentlich bekannt, die bei einer Ausnutzung zu einer Einschränkung der Verfügbarkeit des Webservers führen könnten. Das genaue Patchlevel des Webservers war zum Zeitpunkt der Schwachstellenanalyse nicht bekannt, sodass im schlimmsten Fall davon ausgegangen werden musste, dass der Webserver verwundbar gegenüber dem Angriff ist. Es wurde den Ansprechpartnern empfohlen, zu prüfen, welches Patchlevel im Einsatz ist, um im Anschluss eine Bewertung vornehmen zu können, ob der Webserver tatsächlich verwundbar ist.

In drei der fünf Schwachstellenanalysen konnte zudem identifiziert werden, dass die Webanwendungen JavaScript-Bibliotheken von Drittanbietern einsetzten, die teilweise veraltet und die gegenüber bekannten Schwächen verwundbar sind. In der Regel brachten diese Bibliotheken mögliche Verwundbarkeit gegenüber Cross-Site-Scripting-Angriffen in die Anwendung ein. Hierdurch wäre ein Angreifer in der Lage, Angriffe durchzuführen, wodurch sich z. B. eigener (Schad-)Code in Anfragen platzieren ließe, der dann im Browser von potentiellen Opfern zur Ausführung kommt. JavaScript-Bibliotheken von Drittanbietern kommen in modernen Webanwendungen regelmäßig zum Einsatz. Der Einsatz dieser Art von Software bringt jedoch die Gefahr mit sich, dass die Bibliothek einmalig integriert und dann nicht mehr ausgetauscht wird, wenn Schwächen bekannt oder Updates veröffentlicht werden.

Bei Schwachstellen im Kontext von eingesetzter Software wurde den Ansprechpartnern empfohlen, dass sämtliche im Einsatz befindliche Software, Bibliotheken und Frameworks von Drittherstellern in regelmäßigen Abständen bzw. zeitnah nach dem Bekanntwerden von Schwachstellen aktualisiert werden.

6.2.2 Schwachstellen im Kontext der Upload-Funktionen

Vier von fünf geprüften Portalen wiesen Antragsstrecken mit Upload-Funktionalitäten auf. Im Rahmen der Prüfungen dieser Funktionalitäten konnten in allen Fällen Schwachstellen mit mittlerem Risikograd identifiziert werden, die sich folgendermaßen zusammenfassen lassen:

- In einigen Fällen war es möglich, beliebige Dateiformate hochzuladen oder Einschränkungen der Dateiformate zu umgehen. Hierbei war unter anderem möglich, ausführbare .exe-Dateien hochzuladen, die gefährlich für die entsprechenden Anwendungen werden könnten. In weiteren Fällen war es möglich, Einschränkungen zu umgehen. Beispielsweise ließen einige Anwendungen lediglich den Upload von Bilddateien zu. Durch eine Manipulation der Requests konnten jedoch weitere Dateiformate hochgeladen und diese Einschränkungen so umgangen werden.
- In einigen Fällen konnten sehr große Dateien in sehr kurzer Zeit hochgeladen werden. Dies könnte dazu führen, dass der Speicherplatz des Servers überfüllt wird.
- In vielen Fällen wurde der Upload von Test-Virendateien nicht erkannt, sodass darauf geschlossen werden konnte, dass kein Virenscanner im Einsatz ist. Dies würde es auch einem Angreifer

ermöglichen, schadhafte Dateien auf den Server hochzuladen, die dann im Zuge der Weiterverarbeitung der abgegebenen Anträge zur Ausführung kämen. In einem Fall war bekannt, dass die getestete Antragsstrecke im Nachgang an ein System zur Schadcodeerkennung angeschlossen werden sollte.

Den Service- und Kommunalportalen wurde empfohlen, nur Dateiformate zuzulassen, die explizit erlaubt und vorgesehen sind. Hierbei muss serverseitig eine genaue Prüfung der Datei vollzogen werden. Auch die Größe und Anzahl der durchgeführten Uploads sollte überwacht werden, um eine Überlastung des Servers zu vermeiden. Zusätzlich sollte ein Virenscanner im Einsatz sein, der alle von Bürgerinnen und Bürgern hochgeladenen Dateien überprüft und im Falle von schadhaften Inhalten wieder vom Server entfernt.

6.2.3 Denial-of-Service durch zwischengespeicherte Anträge

Ein getestetes Portal bot eine Funktionalität an, über die Bürgerinnen und Bürger die eingegebenen Daten zwischenspeichern können, um die Bearbeitung des Antrags zu einem späteren Zeitpunkt fortzuführen. Über ein Menü können diese zwischengespeicherten Anträge dann aufgerufen werden. Im Test wurde festgestellt, dass das Abrufen dieser Übersicht bereits bei einer kleinen Anzahl von zwischengespeicherten Anträgen eine deutliche Bearbeitungszeit beim Server hervorruft. Dies deutet an, dass die Darstellung dieser Übersicht eine merkliche Last für den Server generiert. Möglicherweise kann durch ein bösartiges Verhalten eines Benutzers hierüber ein Denial-of-Service provoziert werden, indem kontinuierlich die entsprechende Übersicht aufgerufen wird. Die Schwachstelle wurde mit einem mittleren Risiko bewertet. Den Ansprechpartnerinnen und Ansprechpartnern wurde im Rahmen der Prüfung empfohlen, zu prüfen, inwiefern die Effizienz der betroffenen Funktion verbessert werden kann. Da dies entscheidend von der serverseitigen Implementierung der Anwendung abhängt, konnte hierzu keine allgemeine Empfehlung ausgesprochen werden. Des Weiteren sollte in Betracht gezogen werden, dass die Ausführung der Funktionen überwacht wird, sodass Benutzer nur eine bestimmte Anzahl an Funktionen in einem festgesetzten Zeitraum ausführen oder grundsätzlich nur begrenzt Anträge zwischenspeichern können. Im Nachgang wurde durch die Ansprechpartnerinnen und Ansprechpartner mitgeteilt, dass die Problematik insbesondere auf das untersuchte Testsystem zurückzuführen ist. Dem betrachteten Testsystem stünden, anders als dem Produktivsystem, deutlich weniger Ressourcen zur Verfügung. Ergänzend würden mit einem produktionsnahen Testsystem weitergehende Last- und Performancetests durchgeführt.

6.2.4 Unsichere Weiterleitung beim Login

In einem Portal trat eine unsichere Weiterleitung beim Login als Schwachstelle auf und wurde mit einem mittleren Risikograd gewertet. Wird der Login-Prozess in der Webanwendung durchgeführt, so wird der Benutzer am Ende des Logins auf eine neue Seite weitergeleitet. Die Seite, auf die weitergeleitet wird, wird zu Beginn des Login-Prozesses in einem Übergabeparameter festgelegt. Angreifer könnten diese Links so manipulieren, dass der Anwender den normalen Login-Prozess der Webanwendung durchläuft, aber am Ende zu einer vom Angreifer kontrollierten Webseite weitergeleitet wird. Da zuvor der normale Login-Prozess mit Zwei-Faktor-Authentifizierung durchgeführt wird, ist es wahrscheinlich, dass der Benutzer dieser Seite sein Vertrauen entgegenbringt. Diese Art von Schwachstelle ist als „Open Redirect“ bekannt. Angreifer können diesen Umstand für Phishing-Angriffe verwenden. Den Ansprechpartnern des Portals wurde empfohlen, dass die URL für die Weiterleitung nicht über einen Parameter gesteuert werden sollte, der durch Angreifer manipuliert werden kann. Weiterhin sollte die Anwendung die Angaben im redirect-Parameter daraufhin überprüfen, ob es sich um eine URL handelt, auf die die Anwendung tatsächlich eine Weiterleitung erlaubt. Ist dies nicht der Fall, sollte der Login-Vorgang nicht gestartet werden und der Benutzer nicht auf die angegebene Seite weitergeleitet werden. Zur Umsetzung dieser Überprüfung sollte eine Allow-List verwendet werden, damit exakt spezifiziert ist, welche URLs für die Weiterleitung tatsächlich erlaubt sind.

6.2.5 Umgang mit sensiblen Informationen

In drei von fünf Portalen konnte der Umgang mit sensiblen Informationen als Schwachstelle mit geringem Risikograd identifiziert werden. Sie bezieht sich darauf, dass moderne Browser es Benutzern ermöglichen,

Eingaben in Formularfeldern einer automatischen Rechtschreibprüfung während der Eingabe von Daten zu unterziehen. Dies geschieht entweder durch den Abgleich mit einem lokal im Browser installierten Wörterbuch (einfache Rechtschreibprüfung) oder unter Zuhilfenahme eines meist cloudbasierten Diensts der Browserhersteller (erweiterte Rechtschreibprüfung). Wird ein cloudbasierter Dienst zur Prüfung verwendet, werden diese potentiell sensiblen Daten an Dritte gesendet. Die Vertraulichkeit der in die Anwendung eingegebenen Daten ist daher beeinträchtigt. Ein weiteres Attribut, das für alle Formularfelder mit möglicherweise sensiblen Nutzereingaben gesetzt werden sollte, ist autocomplete="off". Dieses verhindert, dass der Browser einmal getätigte Formulareingaben speichert und diese bei einem erneuten Aufruf der Seite, möglicherweise durch einen anderen lokalen Anwender, vorausfüllt.

6.2.6 Secure-Merkmal im Cookie fehlt

In der Regel wird ein fehlendes Secure-Merkmal als Sicherheitshinweis gewertet. Da jedoch in einem Fall weder das Secure-Merkmal noch HTTP Strict Transport Security (HSTS) gesetzt war, wurde in diesem Fall das fehlende Secure-Merkmal als Schwachstelle gewertet, da bei Aufbau der Kommunikation über HTTP der Inhalt des Cookies unverschlüsselt übertragen worden wäre. Dies kann beispielsweise eintreten, wenn die URL händisch eingegeben wird. Eine detaillierte Beschreibung des Secure-Merkmals und HSTS findet sich in Kapitel 6.2.7.1 und Kapitel 6.2.7.2.

6.2.7 Identifizierte Sicherheitshinweise

Neben den beschriebenen Schwachstellen, die mit Risikograd bewertet wurden, wurden auch Sicherheitshinweise identifiziert.

6.2.7.1 Session Handling

In einzelnen Aufrufen von zwei getesteten Portalen werden Informationen aus dem Cookie auch in der URL übertragen. Da aufgerufene URLs an verschiedenen Stellen protokolliert oder anderweitig gespeichert werden können, kann hierdurch potentiell ein Zugriff auf sensible Informationen durch Dritte möglich sein. Wenn z. B. die URL beim Nachladen externer Ressourcen über den Referer-Header an eine andere Webseite gesendet wird, kann beispielsweise der Betreiber dieser Webseite diese URL einsehen. Im Test gelang es nicht, auf Basis dieser Informationen die Sitzung des Nutzers zu übernehmen, die Tatsache wird daher als Hinweis gewertet. Dennoch wurde den Ansprechpartnern empfohlen, sensible Informationen nicht in der URL zu übertragen.

Drei von fünf Portalen setzten nicht die notwendigen Sicherheitseigenschaften des Cookies. Hierzu gehört zum einen das Secure-Merkmal. Ist dieses nicht gesetzt, so kann das Cookie potentiell auch über einen unverschlüsselten Kanal versendet werden. Dies würde einem Angreifer, der Daten passiv mitlesen kann, erlauben, das übertragene Cookie mitzulesen und so unberechtigten Zugang zur Session eines Benutzers zu erlangen.

Ist das HttpOnly-Merkmal nicht gesetzt, so kann das betroffene Cookie auch durch JavaScript ausgelesen werden. Angreifer könnten hierüber potentiell das Cookie auslesen, was weitere Angriffe vereinfachen kann. Hierzu müsste aber in der Anwendung eine Schwachstelle vorliegen, über die Angreifer eigenen JavaScript-Schadcode ausführen können („Cross Site Scripting“). Eine solche Schwachstelle konnte aber in keiner Prüfung festgestellt werden, weshalb dieser Umstand jeweils nur als Hinweis dokumentiert wurde. Die Verwendung des HttpOnly-Merkmals bleibt aus Sicht des „Defense-in-Depth“-Gedankens dennoch empfehlenswert.

6.2.7.2 Fehlende HTTP-Security-Kopfzeilen (Header)

Während der Prüfungen wurde festgestellt, dass einige Header nicht durch die Portale gesetzt werden. Diese Header würden zusätzlichen Schutz vor Angriffen bieten, da sie Sicherheitsmechanismen in Browsern aktivieren. Das Fehlen der Header erhöht damit die Wahrscheinlichkeit für erfolgreiche Angriffe.

Es wurde festgestellt, dass einige Portale die HTTP Strict Transport Security nicht umsetzten. Mittels HTTP Strict Transport Security (HSTS) weist der Webserver den Browser an, zukünftig nur verschlüsselt über HTTPS mit ihm zu kommunizieren. Zudem wird durch die gängigen Browser fortan das Konfigurieren von Ausnahmen bei fehlerhafter Zertifikatsprüfung verweigert. Wird die Webanwendung mit HSTS-Header einmal aufgerufen, wird der Browser für die in Sekunden gesetzte Dauer alle Aufrufe nur noch verschlüsselt ausführen, selbst wenn der Nutzer „http://“ eingibt. Dies kann zudem für alle Subdomains erzwungen werden.

Weiterhin wurde festgestellt, dass einige Portale keine oder nur eine unsicher konfigurierte Content-Security-Policy (CSP) einsetzten. Durch den Einsatz einer CSP kann durch die Anwendung die Nutzung von Ressourcen (wie z. B. JavaScript oder andere, teilweise aktive Inhalte) in Browsern reglementiert werden. Ferner kann das Einbetten der Webseite in andere Seiten unterbunden werden. So kann das Einbinden fremder Ressourcen oder das Ausführen von eingeschleustem Script-Code durch eine restriktive CSP unterbunden werden, sodass der Browser diese nicht nachlädt oder ausführt. Über die Attribute können sehr differenziert Schutzmechanismen eingesetzt werden. Allerdings haben diese einen erheblichen Einfluss auf die Funktionsweise der Webanwendung. Der Einsatz von CSP-Attributen wird empfohlen, allerdings erfordert die Umsetzung eine sorgfältige Prüfung der Attribute und Parameter.

In einigen Fällen wurde festgestellt, dass der Header „X-Permitted-Cross-Domain-Policies“ nicht gesetzt wurde. Durch diesen können die gültigen Cross-Domain-Policies eingeschränkt werden. Die Cross-Domain-Policy regelt, ob ein Webclient, wie beispielsweise Adobe Flash Player oder Adobe Acrobat, die Daten der Webanwendung im Kontext anderer Domains verarbeiten darf.

Einige der Portale setzten den Referer-Header nicht. Die Referrer-Policy regelt, welche Informationen im Referer-Header übermittelt werden. Bei fehlerhafter Konfiguration kann die gesamte URL (inkl. Parameter) an einen (fremden) Zielserver übermittelt werden.

6.2.7.3 HTTP-Methoden

Ein Webserver erlaubte die Verwendung der HTTP-Methoden TRACE und OPTIONS, die normalerweise hauptsächlich zu Debugging-Zwecken genutzt werden. Mittels der TRACE-Methode werden die an den Webserver gesendeten Daten reflektiert und an den Client zurückgesendet. Mittels der OPTIONS-Methode lassen sich alle nutzbaren HTTP-Methoden anzeigen. Durch den Einsatz von Methoden, die zu Debugging-Zwecken genutzt werden, kann ein Angreifer gegebenenfalls weitere Informationen über ein System sammeln und diese nutzen, um anschließende Angriffe zu präzisieren.

Den Ansprechpartnern wurde empfohlen, diese HTTP-Methoden zu deaktivieren.

7 Fazit und Ausblick

Das Projekt lieferte einen ersten Überblick über den Markt und Einblick in die Sicherheitslage ausgewählter Portale. Aus den gewonnen Erkenntnissen können Betreibende zielgerichtet unterstützt werden und Hilfestellungen in Form von Handlungsempfehlungen erarbeitet werden.

In der Marktanalyse stellte sich heraus, dass es eine große Herausforderung ist, einen Marktüberblick in diesem Bereich zu erstellen. Dies ist auf die Vielzahl an Lösungen auf dem Markt, die aktuell sehr dynamische Lage und die unterschiedliche Herangehensweise zur Umsetzung des OZG zurückzuführen.

Hinsichtlich der Apps für mobile Lösungen wurden in der Marktrecherche Unterschiede in Art und Umfang festgestellt. Die Mehrheit der gefundenen Apps dienen vornehmlich der Informationsprovision und bieten interaktive Funktionen nur in eingeschränktem Maße an. Hier machen sie jedoch Gebrauch von der Mobilität des Endgeräts, etwa im Mängelmelder. Das Stellen von Anträgen über mobile Lösungen hat nachgeordnete Priorität. Hier setzen die meisten Lösungen auf browserbasierte Ansätze, die einen Pflegeaufwand minimieren. Neben Lösungen, die mit einem Nachnutzungsgedanken konzipiert sind, gibt es ebenfalls einen signifikanten Anteil an Individuallösungen. Grundsätzlich ist eine aktive Weiterentwicklung des Funktionsumfangs zu beobachten. Aufgrund des aktuellen Umsetzungsstandes, wurde keine App-Lösung in die Schwachstellenanalysen einbezogen.

Die Marktanalyse der Webportale zeigte den deutlichen Unterschied zwischen Produkten für mobile Endgeräte und Webportalen. Im Gegensatz zu den mobilen Apps bestehen Webportale aus Zusammenschlüssen unterschiedlicher Komponenten, die zu einem individuellen/einzigartigen Portal verknüpft werden. Dementsprechend gestaltete sich die Informationsgewinnung hier deutlich komplexer/aufwendiger. Durch Internet-Recherche und Fragebogen wurde ersichtlich, dass der größte Informationsgewinn durch den direkten Kontakt erfolgen kann. Als begünstigender Faktor erwies sich hier ein Vertrauensanker entweder durch bestehenden Kontakt aus vorherigen Veranstaltungen, oder über thematische Netzwerke.

Im Anschluss an verschiedene Gespräche mit Betreibenden wurden fünf Portale ausgewählt, die einer Schwachstellenanalyse unterzogen wurden.

Die Planung und das Scoping der einzelnen Schwachstellenanalysen gestalteten sich umfangreicher als angenommen. Dies lag insbesondere daran, dass viele Parteien in die Entwicklung und den Betrieb der einzelnen Portale involviert sind und die Portale mit diversen weiteren Schnittstellen (beispielsweise Integrationsdienste) kommunizieren. Da Schwachstellenanalysen auch bei abwägender Vorgehensweise gewisse Risiken mit sich bringen könnten, war es hierbei sehr wichtig, alle Ansprechpartner und Ansprechpartnerinnen über die Schwachstellenanalysen zu informieren und mögliche Auswirkungen bereits im Vorfeld zu besprechen.

Im Rahmen von Schwachstellenanalysen werden in vielen Fällen – auch in diesem Projekt – vorrangig die über das Internet erreichbaren Weboberflächen und die von diesen direkt angesprochenen Schnittstellen untersucht. Für einen ersten Überblick ist diese Vorgehensweise durchaus sinnvoll. Werden jedoch regelmäßige Schwachstellenanalysen ausgeführt, hat es in vielen Fällen Sinn, den Blickwinkel auch zu verändern und weitere Schnittstellen im Rahmen der Analysen zu betrachten. Dies ermöglicht einen deutlich breiteren Blick auf die Sicherheit des jeweiligen Portals.

In allen fünf durchgeführten Schwachstellenanalysen konnten Schwachstellen in der Infrastruktur oder der Anwendung identifiziert werden. Positiv ist hier hervorzuheben, dass hierbei keine Schwachstellen mit hohem oder kritischem Risikograd aufgetreten sind. Das Projekt war jedoch auf eine Zusammenarbeit mit den jeweiligen Portalbetreibern angewiesen und betrachtete einen gemeinsam abgestimmten Scope. Alle Testgegenstände, die im Rahmen des Projekts betrachtet wurden, sind bereits in der Vergangenheit mehrfach Schwachstellenanalysen unterzogen worden.

Systemseitig konnten im Rahmen der Schwachstellenanalysen vor allem Probleme mit der TLS-Konfiguration identifiziert werden. Grundsätzlich empfiehlt das Projektteam hier eine Anpassung der TLS-

Konfigurationen, sodass durch den Web-Server nur die in den entsprechenden Richtlinien empfohlenen Protokolle und Cipher Suites angeboten werden. Weiterhin wird Betreiberinnen und Betreibern empfohlen zu prüfen, ob lediglich Cipher Suites mit dem ECDHE-Schlüsselaustausch (EC = „Elliptic Curve“) angeboten werden können.

Aus den Prüfungen der Anwendungen kann insbesondere das Fazit gezogen werden, dass vor allem Upload-Funktionen einen großen Risikofaktor für Anwendungen im Bereich des OZG-Kontextes darstellen. Können Bürgerinnen und Bürger über Upload-Funktionen eigene Dateien auf Server hochladen, muss hierbei darauf geachtet werden, dass diese Dateien als potentiell gefährlich einzustufen sind und vor einer Weiterverarbeitung überprüft werden müssen.

Die verwendete Anwendungssoftware und die eingesetzten Software-Bibliotheken aktuell zu halten, ist für Betreiberinnen und Betreiber stets eine Herausforderung. Bei den durchgeführten Schwachstellenanalysen wurde verifiziert, dass in nahezu allen Fällen die Applikationssoftware auf dem aktuellen Stand war. Lediglich in einem Fall konnte hier eine Verwundbarkeit im Kontext des eingesetzten Webservers identifiziert werden. Im Fall der verwendeten Softwarebibliotheken konnten in einigen Portalen veraltete oder verwundbare Bibliotheken identifiziert werden. Dies bezieht sich vor allem auf eingesetzte JavaScript-Bibliotheken, die durch die Verantwortlichen aktualisiert werden sollten.

Im Rahmen der Schwachstellenanalysen konnte so zum einen nachgewiesen werden, dass die jeweiligen Ansprechpartner und Ansprechpartnerinnen mit dem Themengebiet „Schwachstellenanalysen“ sehr vertraut sind. Weiterhin konnte durch das im Schnitt recht hohe Sicherheitsniveau auch identifiziert werden, dass die regelmäßig durchgeführten Schwachstellenanalysen aufseiten der Portale für eine Verbesserung der IT-Sicherheit sorgen. Alle untersuchten Portale wiesen ein mittleres bis hohes Sicherheitsniveau auf. Es wird daher allen Herstellern und Betreibern von Service- und Kommunalportalen – aber auch anderen Anwendungen im OZG-Kontext und darüber hinaus – empfohlen, regelmäßig Sicherheitsüberprüfungen durchzuführen und IT-Sicherheit direkt in den Entwicklungszyklus zu integrieren, um eine nachhaltige Verbesserung der IT-Sicherheit erreichen zu können.

Es sei an dieser Stelle darauf hingewiesen, dass es das Ziel dieses Projekts war, einen Überblick über aktuelle Umsetzung und Sicherheitslage der Portale zu erhalten, um identifizieren zu können, wie die sichere Umsetzung unterstützt werden kann. Ein vollumfänglicher Test der OZG-Landschaft konnte im Rahmen dieses Projekts jedoch nicht erfolgen. Es kann keine Aussage über die Sicherheitseigenschaften der Portale getroffen werden, die nicht Bestandteil der Überprüfungen waren.

Die Ergebnisse der Marktanalyse und der Schwachstellenanalysen sowie die daraus abgeleiteten Erkenntnisse dienen als Informationsbasis zur Erarbeitung von Handlungsempfehlungen und Technischen Richtlinien, insbesondere der BSI TR-03172 Portalverbund, sowie als Unterstützung der sicheren Gestaltung der OZG-Umsetzung.

8 Anhang: Fragebogen

Nachfolgender Fragebogen wurde im Rahmen der Marktrecherche an die OZG-Koordinatorinnen und OZG-Koordinatoren sowie die Ansprechpartnerinnen und Ansprechpartner der Themenfelder übersendet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der IT-Sicherheitsdienstleister secuvera führen aktuell eine Markt- und Schwachstellenanalyse zur Sicherheit von E-Gov-Webportalen und -Apps durch (MaSiGov). Ziel dieser Marktanalyse ist es, herauszufinden, welche Softwarelösungen für E-Government-Portale (Webportale und mobile Apps) aktuell am Markt existieren und wie weit diese verbreitet sind.

Im weiteren Projektverlauf werden ausgewählte Produkte detaillierter untersucht, insbesondere auch auf technische Schwachstellen. Unser gemeinsames Ziel in diesem Projekt ist es, einen Überblick über das Sicherheitsniveau der einzelnen Produkte zu erlangen sowie infolgedessen die Sicherheit der Bürger-Daten beurteilen zu können. Im Rahmen eines Coordinated-Vulnerability-Disclosure-Prozesses ist es ebenso unser Ziel, Schwachstellen frühzeitig zu identifizieren und zu unterstützen, sodass gefundene Schwachstellen durch die Hersteller nachhaltig beseitigt werden können.

Da Sie sich bereits sehr intensiv mit Produkten im E-Government-Portalbereich beschäftigt haben, würden wir uns freuen, wenn wir von Ihrem Know-how profitieren könnten, und möchten Sie daher bitten, den angehängten Fragebogen auszufüllen. Wir würden uns ebenfalls freuen, wenn Sie den Fragebogen an weitere interessierte Kommunen weiterleiten würden – jeder beantwortete Fragebogen hilft uns in unserer Marktrecherche sehr weiter.

Allgemeine Fragen

1. *Welche Produkte haben Sie aktuell im Einsatz (Webportale, native Apps für mobile Geräte)?*

2. *Wurde das Produkt selbst entwickelt oder über einen Hersteller eingekauft?*

3. *Welche weiteren Produkte haben Sie im Rahmen des Auswahlprozesses betrachtet oder sogar getestet?*

4. *Gab es einzelne Funktionen, die für die Verwendung des aktuellen Produktes ausschlaggebend waren? Wenn ja: Welche sind diese?*

5. *Welche Funktionen haben sich bei der täglichen Verwendung als essentiell herausgestellt?*

6. *Handelt es sich bei Ihrem Produkt um eine modular aufgebaute Software? Falls ja, nutzen Sie den vollen Funktionsumfang oder wurden einzelne Module ausgewählt?*

7. *Auf einer Skala von 1-5: Wie zufrieden sind Sie mit den aktuell verwendeten Produkten? (1: sehr zufrieden; 5: sehr unzufrieden)*

IT-Sicherheit und Datenschutz

8. *Wurden bei der Auswahl die Aspekte Datenschutz und IT-Sicherheit betrachtet?*

   Ja ☐ Nein ☐ Raum für Erläuterungen: _____

9. *Wurde bei der Auswahl des Produktes Ihr Datenschutzbeauftragter konsultiert?*

   Ja ☐ Nein ☐ Raum für Erläuterungen: _____

10. *Gab es vorab festgeschriebene Anforderungen bezüglich IT-Sicherheit? Falls ja, welche?*

11. *Auf einer Skala von 1-5: Wie wichtig war IT-Sicherheit im Rahmen des Auswahlprozesses? (1: sehr wichtig; 5: sehr unwichtig)*

E-Government

12. *Wie ist die Bürger-Authentifizierung in Ihrer Lösung umgesetzt? Nutzen Sie eine Lösung, die für E-Government geeignet ist? Wenn ja, welche?*

13. *Inwiefern war eine E-Government-Eignung bereits bei der Auswahl des Produkts ein Kriterium für Sie?*

14. *Falls E-Government bisher noch kein Teil der Lösung ist, planen Sie dies in naher Zukunft zu ändern?*

Abkürzungsverzeichnis

Abkürzung	*Beschreibung*
apk-Datei	Android Package-Datei
ASVS	Application Security Verification Standard
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSS	Cascading Style Sheets
HTML	Hypertext Markup Language
MaSiGov	Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Apps und Webportalen
OWASP	Open Web Application Security Project
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, Onlinezugangsgesetz
PoI	Points of Interest
SQL	Structured Query Language
TR	Technische Richtlinie
UI	User Interface

Tabelle 7: Abkürzungen

Glossar

Bezeichnung	*Beschreibung*
Angriffskatalog	Liste aller Testszenarien, die im Rahmen der Schwachstellenanalysen durchgeführt werden können.
Authentisierung	Eine Authentisierung bezeichnet den Nachweis einer Identität mithilfe von geeigneten Faktoren, beispielsweise dem Wissen eines geheimen Passworts.
App-Store	Eine digitale Vertriebsplattform, über die vor allem mobile Anwendungen für Smartphones und Tablets bereitgestellt werden.
Black-Box-Test	Schwachstellenanalysen, die ohne Kenntnisse der zu prüfenden Umgebung, z. B. nur mit Kenntnis der Adresse eines Zielsystems, durchgeführt werden. Diese Angriffsform versucht die Sichtweise eines externen Angreifers ohne Kenntnisse interner Strukturen einzunehmen. Das Gegenteil ist der White-Box-Test.
Burp Suite Professional	Prüfwerkzeug mit automatisierten und halb-automatisierten Methoden zur Prüfung von Webanwendungen und Kommunikation.
Business Logic	Eine Prüfkategorie des Testkatalogs, in dem Prüfungen der Geschäftslogik der Anwendungen beschrieben werden.
Cipher Suite	Eine Cipher Suite ist eine Sammlung kryptografischer Algorithmen zur Verschlüsselung von Nachrichten.
Denial-of-Service-Angriff	Eine Angriffstechnik, die zu einer Einschränkung der Verfügbarkeit einer Anwendung oder eines Dienstes führt.
Desktop-App	Eine App, die nicht auf einem mobilen Client installiert wird, sondern auf einem Laptop oder ein Desktop-PC.
Diffie-Hellman Ephemeral	Ein Schlüsselaustauschverfahren im Kontext von Transportverschlüsselung.
Durchführungskatalog	Auf Basis des Angriffskatalogs wurde je geprüftes Portal ein Katalog an konkreten Tests erstellt, die im Rahmen der Prüfung durchgeführt wurden. Dieser Katalog mit konkreten Testfällen nennt sich Durchführungskatalog.
Elliptic Curve Diffie-Hellman Ephemeral	Ein Schlüsselaustauschverfahren im Kontext von Transportverschlüsselung, welches elliptische Kurven verwendet.
eID-Funktion	Funktion zum elektronischen Identitätsnachweis
Front-End	Die Benutzeroberfläche, die Anwender im Browser verwenden.
Native Apps	Native Apps benötigen im Gegensatz zu den Webportalen keinen Browser. Sie laufen daher vollumfänglich auf dem mobilen Endgerät.
nmap	Ein Werkzeug um Portscans auf Systemen durchführen zu können.
Information Gathering	Ziel einer Informationsgewinnung ist es, so viele Informationen wie möglich über ein Zielsystem zu sammeln, welche im nächsten Schritt für Angriffe verwendet werden können.
Input Validation	Überprüfung und Bereinigung von Benutzereingaben.

Bezeichnung	*Beschreibung*
JavaScript-Bibliothek	Eine Bibliothek von Funktionen mit vorgefertigtem JavaScript-Code, die es Entwicklern ermöglichen auf bereits vorhandene Funktionalitäten zuzugreifen.
Negativ-Reporting	Eine Beschreibung aller Testfälle, die durchgeführt wurden, auch wenn die Prüfungen zu keiner Schwachstelle geführt haben.
OpenVAS	Ein Schwachstellenscanner, mit dessen Hilfe Systeme auf bekannte Schwachstellen geprüft werden können.
OWASP Web Security Testing Guide	Ein Testkatalog für Webanwendungen zur Durchführung von Schwachstellenanalysen des Open Web Application Security Projects.
Patchlevel	Der aktuelle Stand eines Systems, der festhält, welche Updates bereits eingespielt wurden.
Progressive Apps	Progressive Apps, die sich als Kompromiss zwischen responsiver Webseite und nativer App beschreiben lassen, verwenden für den Aufruf ebenfalls einen Browser
Scope	Beschreibung des Fokus der Schwachstellenanalyse.
testssl	Ein Testwerkzeug für die Prüfung von Verbindungen, die mithilfe einer Transportverschlüsselung abgesichert sind.
sqlmap	Ein Testwerkzeug für die Suche nach SQL-Injection Schwachstellen.
TLS	Transport Layer Security, ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet
Upload-Funktion	Eine Funktion zum Hochladen z. B. eines Dokuments innerhalb einer Webanwendung
White-Label-Lösung	Diese Art von Lösungen stellt grundsätzliche Anwendungslogik bereit. Sie lässt sich aber durch Betreiber oder andere Hersteller weiter personalisieren und verändern.
Zwei-Faktor-Authentisierung	Hierbei handelt es sich um eine Authentisierung, in der zwei voneinander unabhängige Faktoren, etwa „Wissen“ und „Besitz“ erforderlich sind. Ein Beispiel hierfür ist die Kombination aus Passwort (Wissen) und mTAN (Besitz der SIM-Karte).

Tabelle 8: Glossar

Literaturverzeichnis

[1] „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG) vom 14.08.2017," [Online].

[2] J. Bager, T. Gerber und C. Wölbert, „Halbdigital - Digitalisierung der Verwaltung: eine Bestandsaufnahme,"
c't, Nr. 6, pp. 60-64, 2022.

[3] „Darstellung des OZG-Reifegradmodells," [Online]. Available: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-reifegradmodell/info-reifegradmodell-node.html.

[4] Open Web Application Security Project Foundation, „OWASP Web Security Testing Guide," [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/.

[5] Open Web Application Security Project Foundation, „OWASP Application Security Verification Standard (ASVS)," [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/.

[6] Bundesamt für Sicherheit in der Informationstechnik, „Studie: Durchführungskonzept für Penetrationstests," 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3.

[7] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS)," 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html.

[8] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen," 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html.