secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

ABSCHLUSSGUTACHTEN

VERSION 1.0 | 02.07.2020

Gutachten im Auftrag der Bundesrechtsanwaltskammer – Körperschaft des öffentlichen Rechts
Littenstraße 9
10179 Berlin

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden/Stuttgart

INHALTSVERZEICHNIS

1. MANAGEMENT SUMMARY

1.1. Zielsetzung

Die Firma secuvera GmbH (secuvera) wurde von der Bundesrechtsanwaltskammer (BRAK) beauftragt, eine IT-Sicherheitsprüfung der Fortschreibung des Systems „besonderes elektronisches Anwaltspostfach“ (beA) im Zuge eines Betriebsübergangs an eine neue Betreiberin durchzuführen. Die neue Betreiberin des beA ist die WesRoc GbR, die ein Konsortium bestehend aus der Westernacher Solutions GmbH und der Rockenstein AG darstellt.

Eine grundsätzliche IT-Sicherheitsprüfung des beA wurde durch die Firma secunet im Jahr 2018 nach Veröffentlichungen zu Schwachstellen im System durchgeführt und mit einem Gutachten an die BRAK übergeben. Im Rahmen der Überprüfung wurde auch die Dokumentation der Informationssicherheit betrachtet. Diese Überprüfung führte zu Anmerkungen und Befunden.

Auf Grundlage des Gutachtens der secunet wurde das Sicherheitsregelwerk bestehend aus

- IT-Sicherheitskonzept,
- Betriebssicherheitskonzept,
- Kryptokonzept,
- Incident- und Security-Management-Konzept und
- Schlüsselmanagement

zusammengestellt bzw. überarbeitet. Hierbei wurden die im Gutachten adressierten Punkte so aufgegriffen, dass für die darauf aufbauende Betriebsphase ein geeigneter Stand der Dokumentation erreicht wurde. Die secunet AG stellte nach erneuter Vorlage der Dokumente fest, dass diese geeignet seien, die wesentlichen Sicherheitsmaßnahmen des beA zu erläutern und den gewünschten Nachweis hinreichender Sicherheit der Funktionen des beA zu liefern.

Das Ziel der vorliegenden IT-Sicherheitsprüfung liegt nun darin, im Rahmen des Betriebsübergangs eine bessere und nachhaltigere Basis für die Beschreibung des Sicherheitskonzepts und für die Umsetzung der Sicherheitsmaßnahmen zu erreichen. Der Auftrag der Sicherheitsprüfung sah hierzu vor, dass sich die Untersuchungen von April bis Ende Mai 2020 auf die fortgeschriebenen bzw. angepassten Anteile des IT-Sicherheitskonzepts und der darin aufgeführten Sicherheitsmaßnahmen beziehen. Die Aufrechterhaltung eines gleichbleibend hohen Sicherheitsniveaus sollte ebenfalls überprüft werden. Die IT-Sicherheitsprüfung umfasste auftragsgemäß keine Betrachtung der Clientkomponenten oder des Verschlüsselungskonzepts, sondern ausschließlich den Betrieb der zentralen Infrastruktur.

Die IT-Sicherheitsprüfung umfasste die folgenden Anteile:

- Dokumentenprüfung
  Die durch die neue Betreiberin übernommenen Dokumente des Sicherheitsregelwerks wurden durch diese fortgeschrieben und auf die neu errichtete Betriebsumgebung des beA angepasst. Es sollte geprüft werden, ob durch die Fortschreibung mindestens ein im Vergleich zum vorherigen Betreiber gleichbleibendes Sicherheitsniveau aufrechterhalten wurde.
- Audit und Konfigurationsprüfung
  In einem Vor-Ort-Audit wurde zum einen geprüft, ob die dokumentierten organisatorischen Sicherheitsmaßnahmen bei der neuen Betreiberin umgesetzt werden. Zum anderen wurden im Rahmen von Konfigurationsprüfungen die technischen und betrieblichen Abläufe geprüft.
- Externe technische Prüfung
  Die öffentlichen über das Internet erreichbaren Schnittstellen wurden einer technischen Prüfung aus der Sicht eines anonymen Angreifers unterzogen. Dabei wurden in enger Abstimmung mit der Betreiberin die bestehenden vorgelagerten Sicherheitsmechanismen

zur reaktiven Angriffsabwehr (Intrusion Detection) während des Prüfungszeitraums selektiv deaktiviert, um in kurzer Zeit eine bessere Prüftiefe zu ermöglichen und gleichzeitig eine Aussage über die Resilienz der Infrastruktur ohne vorgelagerte dynamische Angriffserkennung zu erhalten.

Zur Dokumentation der Ergebnisse wurde vom Auftraggeber um die Erstellung eines Abschlussgutachtens gebeten, das mit diesem Dokument an die Bundesrechtsanwaltskammer übergeben wird. In diesem Abschlussgutachten wird der Stand zum Zeitpunkt der jeweiligen Prüfungsschritte abgebildet. Während der Analyse festgestellte Schwachstellen und Befunde wurden soweit möglich schon vor Fertigstellung dieses Gutachtens an die Betreiberin und den Auftraggeber kommuniziert. Ein Teil der gemeldeten Feststellungen wurde daraufhin durch die neue Betreiberin behoben und konnte erneut durch die Gutachter analysiert werden. Zum Stichtag ist die Behebung von Schwachstellen und Befunden durch die neue Betreiberin bzw. eine erneute Analyse noch nicht abgeschlossen. Soweit verfügbar, sind entsprechende Hinweise zu schon erzielten Verbesserungen in diesem Gutachten vermerkt.

Die Bewertung der Befunde und Schwachstellen erfolgte in folgenden Kategorien:

- Verbesserung,
- Anmerkung,
- Niedrig,
- Mittel,
- Hoch oder
- Kritisch.

Das Vorgehen zur Einteilung der Befunde und Schwachstellen in die aufgelisteten Kategorien wird in Kapitel 2 dargestellt. Hierbei wird auch eine Zuordnung zu den vorangegangenen Bewertungskategorien der secunet abgebildet.

Schwachstellen der Kategorien „Verbesserung“, „Anmerkung“, „Niedrig“ und „Mittel“ werden in den nachfolgenden Kapiteln aufgrund der geringen Priorität nur überblicksweise dargestellt. Die restlichen Kategorien werden ausführlicher erläutert.

Die Inhalte und Ergebnisse der Analysen werden im folgenden Unterabschnitt zuerst überblicksweise dargestellt und in den nachfolgenden Kapiteln ausführlich erläutert.

1.2. Ergebnisse der Dokumentenprüfung

Gegenstand der Dokumentenprüfung war das durch die zukünftige Betreiberin fortgeschriebene und vorgelegte Sicherheitsregelwerk sowie weitere Dokumente, die die Architektur, die betriebliche Basis und die Abläufe des Betriebs näher erläutern. Die Bestandteile des Sicherheitsregelwerks wurden in Kapitel 1.1. bereits aufgeführt.

Überwiegend wurde die Dokumentenprüfung durch eine Analyse der Dokumentenlage der vorgelegten Dokumente durchgeführt. Hierzu wurde die Version der bisherigen Betreiberin als Grundlage angenommen und negative Veränderungen bzw. aktuell für den Betriebsübergang als unzureichend zu bewertende Dokumentationsanteile als Befunde aufgenommen. Die Befunde wurden der Betreiberin und dem Auftraggeber in geeigneter Form zeitnah übermittelt.

Grundsätzlich konnte bei der Dokumentenprüfung ein im Vergleich zur bestehenden Umgebung gleichbleibendes Sicherheitsniveau festgestellt werden. Vereinzelt sind jedoch Nachbesserungen technischer und beschreibender Art durch die neue Betreiberin notwendig.

In der Dokumentprüfung wurden folgende Befunde festgestellt:

Tabelle 1: Statistik der Befunde der Dokumentenprüfung

Kategorie	Anzahl Befunde	davon Anzahl behobener Befunde
Kritisch	0	0
Hoch	6	5 (3 vollständig/2 teilweise)
Mittel	3	1 vollständig
Niedrig	0	0
Anmerkungen	0	0
Verbesserung	2	0

Nach den erwähnten Bewertungskriterien wurden keine kritischen und damit betriebsverhindernden Befunde gefunden.

Als betriebsbehindernd wurde das unzureichende Berechtigungs- und Identitätsmanagement bewertet. Darüber hinaus haben sich überwiegend Befunde ergeben, die sich auf die Struktur oder Aktualität der Dokumente bezogen, nicht aber auf die Prozesse selbst.

Für eine genaue Beschreibung der Befunde wird auf Kapitel 3. verwiesen.

1.3. Ergebnisse der Umsetzungsprüfung

Für den geplanten Betreiberübergang wurden durch die BRAK Konfigurationsprüfungen von geänderten Komponenten und IT-Systemen, Analysen von grundlegenden Betriebsabläufen bei der neuen Betreiberin sowie eine Umsetzungsprüfung der beA-spezifischen Sicherheitsanforderungen im Rahmen eines Audits beauftragt. Für die Prüfungen wurden bereits festgestellte Ergebnisse der Dokumentenprüfung genutzt, um Prüfziele daran auszurichten. Dabei wurden auch Verbesserungshinweise basierend auf der geprüften betrieblichen Dokumentation genutzt, um die aktuelle Betriebsumgebung und die bei WesRoc hierzu etablierten Abläufe zu hinterfragen.

Diese Prüfungen wurden an zwei Tagen Ende Mai 2020 durch Interviews und durch eine Inaugenscheinnahme der Konfiguration der Komponenten und IT-Systeme bei der neuen Betreiberin durchgeführt.

Während des Audits und der Prüfung der Konfigurationen wurde auf bereits vorliegenden Befunden der Dokumentenprüfung und der externen technischen Prüfung aufgebaut. Die Umsetzungsprüfung wurde zur Konkretisierung der Befunde aus der Dokumentenprüfung und der externen technischen Prüfung genutzt. Es konnten hierbei zusammenfassend Befunde mit nachfolgender Ausprägung gefunden werden:

Tabelle 2: Statistik der Befunde der Konfigurationsprüfung

Kategorie	Anzahl Befunde	davon Anzahl behobener Befunde
Kritisch	0	0

Kategorie	Anzahl Befunde	davon Anzahl behobener Befunde
Hoch	0	0
Mittel	3	2 (1 vollständig/1 teilweise)
Niedrig	0	0
Anmerkungen	0	0
Verbesserung	1	1 vollständig

Nach erwähnten Bewertungskriterien wurden daher keine betriebsverhindernden Befunde gefunden.

Es wurden betriebsbehindernde Schwächen und Befunde festgehalten, die sich vor allem auf die Dokumentation und nicht die Prozesse selbst bezogen haben. Zusätzlich wurden Befunde identifiziert, die sich aus der zum Zeitpunkt der Prüfung herrschenden Transitionsphase ergeben haben.

Für eine genaue Beschreibung der Befunde wird auf Kapitel 4. verwiesen.

1.4. Ergebnisse der technischen Prüfung

Wie in der Zielsetzung dargestellt, wurden die Prüfungen aufgeteilt in Prüfungen auf System- und auf Anwendungsebene im Internet erreichbarer Endpunkte der zentralen Infrastruktur. Die Ergebnisse werden nachfolgend zusammengefasst.

Bei den Prüfungen auf Systemebene wurden zwei Schwachstellen identifiziert, die mit CVSS-Risikograd „None“ (Kategorie Anmerkung) bewertet wurden. Daher lässt sich allen geprüften Systemanteilen ein sehr hohes Sicherheitsniveau attestieren.

Die Konfiguration der Transportdatenverschlüsselung mittels TLS weicht auf allen geprüften Adressen von den Empfehlungen der BSI-TR-02102 Teil 2 ab. Daraus ergibt sich jedoch keine ausnutzbare Schwachstelle. Es wird empfohlen, die Konfiguration entlang den Empfehlungen der BSI-TR anzupassen, um das Sicherheitsniveau zu steigern.

Die Firewall meldet bei einer geprüften Adresse einen geschlossenen Port. Dies ist ein Indiz dafür, dass hier zu einem vorigen Zeitpunkt ein Dienst aktiv war, die Konfiguration des Firewall-Regelwerks nach dessen Deaktivierung jedoch nicht angepasst wurde. Damit wird die Kommunikation nicht durch die Firewall, sondern durch das Endsystem unterbunden. Es wird empfohlen, das Regelwerk zu aktualisieren. Ferner meldet ein vorgelagertes System einen UDP-Port aktiv als „nicht erreichbar“. Dies wird hier aufgeführt, da es sich beim meldenden System nach Recherche des Prüfers um eines des Dienstleisters Rockenstein AG handelt. Hier sollte der Sachverhalt analysiert und auch das Firewall-Regelwerk angepasst werden, sodass die Anfrage nicht aktiv beantwortet wird.

Die Schwachstellen wurden nach der Reaktivierung der dynamischen Sicherheitsmechanismen erneut überprüft. Dadurch ergaben sich keine Änderungen an den festgestellten Problemen.

Bei den Prüfungen auf Anwendungsebene konnten insgesamt zwei Schwachstellen identifiziert werden, beide Schwachstellen besitzen einen mittleren CVSS-Risikograd. Aufgrund der Verwendung der JavaScript-Bibliothek jQuery, die veraltet und gegenüber bekannten Schwachstellen verwundbar ist, entsteht eine der beiden Schwachstellen. Die zweite Schwachstelle entsteht, weil den Anwendungen einzelne die Resilienz stärkende HTTP-Kopfzeilen fehlten. Diese Schwäche wurde im Verlauf der Erstellung des Gutachtens behoben und die Behebung durch den Prüfer verifiziert.

In der Prüfung der technischen Umsetzung konnten zusammenfassend Schwachstellen mit nachfolgender Ausprägung gefunden werden:

Tabelle 3: Statistik der Schwachstellen der externen technischen Prüfung

Kategorie	Anzahl Schwachstellen	Davon Anzahl behobener Schwachstellen
Kritisch	0	0
Hoch	0	0
Mittel	2	1
Niedrig	0	0
Anmerkungen	2	0
Verbesserung	0	0

1.5. Resümee und Empfehlung

Alle für die Prüfung angeforderten Informationen wurden bereitgestellt bzw. ein definierter Status zeitnah durch die neue Betreiberin übermittelt. Die betriebliche Infrastrukturumgebung ist von hoher Güte und für die Rechenzentren liegen branchenübliche Zertifizierungen wie TüViT Trusted Site Infrastructure (TSI) vor. Die diesbezüglichen Abläufe sind auf einem sehr belastbaren Sicherheitsniveau ausgeprägt.

Im Rahmen des Betriebsübergangs kommt im Bereich der Entwicklung und Bereitstellung der Betriebsentitäten eine leistungsfähigere und höher automatisierte Arbeitsweise zum Einsatz. Durch die hierbei eingebrachten höheren Standards wird insgesamt ein höheres Sicherheitsniveau und eine flexiblere Anpassungsfähigkeit erreicht.

Die Transition zielte bzgl. der Ablauf- und Anwendungslogik vorrangig auf eine unveränderte Übernahme des Betriebs durch die neue Betreiberin ab. Es sollte funktional und sicherheitstechnisch derselbe Stand beibehalten werden. Die Sicherheitsdokumentation wurde aus diesen Gründen nur an entscheidenden Stellen angepasst. Es war einerseits ersichtlich, dass durch die Betreiberin noch kein länger etabliertes und zertifiziertes ISMS zum Zeitpunkt der Prüfung gegeben war. Die Prüfung konnte an dieser Stelle gezielte Impulse setzen und Verbesserungsmöglichkeiten aufzeigen, die in den aktuellen und zielgerichteten Prozess der ISMS-Zertifizierung einfließen werden. Andererseits wurden durch den Betreiberwechsel schon technische und betriebliche Strukturen und Lösungen eingebracht, die auch bezüglich der Informationssicherheit eine aktuelle und hochgradig automatisierte Basis für den sicheren Betrieb ermöglichen.

Besonders auffallend war das – sowohl dokumentarisch wie auch technisch – unzureichende betriebliche Berechtigungs- und Identitätsmanagement mit verschiedenen Ausprägungen. Dieses wurde durch die neue Betreiberin erkannt und noch während der Prüfung in großen Teilen behoben. Es konnte aufgezeigt werden, dass durch beA-spezifische Schutzmaßnahmen für die Betriebsumgebung keine Auswirkung auf die Anwendung oder die Sicherheit der verarbeiteten Informationen besteht.

Ein bedeutender Teil der Befunde adressiert dem Betriebsübergang zuzuordnende Punkte, die sowohl zur Aufrechterhaltung eines gleichwertigen Sicherheitsniveaus erforderlich sind, als auch in

der Umsetzung und Fortführung auf eine angestrebte Verbesserung abzielen. Im Ergebnis wird die Prüfung mit der begründeten Aussicht auf ein verbessertes und konsolidiertes Sicherheitsniveau abgeschlossen.

Zusammenfassend konnte im Rahmen der Prüfung kein Risiko für die Sicherheit der beA-Anwendung durch den Betriebsübergang identifiziert werden. Eine zielgerichtete und weitere Bearbeitung der noch offenen Befunde sollte entsprechend einer dafür geeigneten Priorisierung gewährleistet werden.

1.6. Abgrenzung

Bei Verwendung dieses Gutachtens sind folgende Hinweise zu beachten:

- Die durchgeführte IT-Sicherheitsprüfung kann nur als stichprobenhafte Überprüfung verstanden werden, in der versucht wurde, mit einem vertretbaren Aufwand mögliche Schwachstellen im Untersuchungskontext zu identifizieren.
- Die Ergebnisse müssen stichtagsbezogen betrachtet werden.
- Der Untersuchungsgegenstand bestand in der Fortschreibung des Sicherheitsregelwerks und technischen Umsetzung seitens der neuen Betreiberin. Die Anwendungslogik ist hierbei in weiten Teilen gleich geblieben und wurde nicht erneut auf technische oder organisatorische Schwachstellen der Nutzung bzw. des Ablaufs hin geprüft.
- Einzelne Befunde zielen auf eine Verbesserung des bestehenden Regelwerks ab. Dies ergibt sich aus den Rahmenbedingungen, die durch den Betriebsübergang und damit verbundenen Zielen bestehen.
- Eine Prüfung der angewendeten Methodik für das Sicherheitsregelwerk wurde nicht vorgenommen. Hinweise zur Verbesserung wurden jedoch aufgenommen.
- Eine Analyse, ob das beA-System alle rechtlichen und über die Sicherheit hinausgehenden funktionalen Anforderungen erfüllt, war nicht Gegenstand der Betrachtung.
- Ergänzend wurden Anteile der betrieblichen Dokumentation und die Querbezüge zum Sicherheitsregelwerk geprüft. Das Prüfziel bestand aber nicht in einer systematischen Prüfung des Betriebs und der dafür dokumentierten Anteile.

Die technische Prüfung wurde auf einer Staging-Umgebung durchgeführt. Mögliche betriebliche Anpassungen für die Produktivumgebung konnten daher prinzipbedingt nicht unmittelbar geprüft werden, sondern ergeben sich aus dem Analogieschluss der Vergleichbarkeit der Umgebungen.

2. VERFAHREN ZUR BEFUND- UND SCHWACHSTELLENBEWERTUNG

In diesem Kapitel wird beschrieben, wie die Darstellung von Befunden und Schwachstellen in den folgenden Kapiteln erfolgt und wie die Einordnung in die Risikostufen durchgeführt wurde.

2.1. Unterscheidung zwischen Befund und Schwachstelle

Zur einfacheren Unterscheidung zwischen Ergebnissen der Dokumentenprüfung, Umsetzungsprüfung durch Audit und Konfigurationsprüfung und der externen technischen Prüfung wird nachfolgend zwischen Befunden und Schwachstellen unterschieden.

Als „Befund" werden hierbei die Ergebnisse der Dokumentenprüfung und der Umsetzungsprüfung durch Audit und Konfigurationsprüfung bezeichnet. Als „Schwachstelle" gelten die Ergebnisse der externen technischen Prüfung.

Zur besseren Referenzierung werden Befunde und Schwachstellen jeweils mit im Dokument fortlaufendem und damit eindeutigem Index versehen. Hierbei wird die nachfolgende Nomenklatur verwendet:

- B_ Befund aus Dokumentenprüfung, Umsetzungsprüfung, Audit oder Konfigurationsprüfung,
- S_ Schwachstellen bei Systemprüfungen und
- W_ Schwachstellen bei Webanwendungsprüfungen.

2.2. Befund

2.2.1. Darstellungsform

Folgende Darstellungsform wurde für die identifizierten Befunde der Kategorien „Kritisch" und „Hoch" gewählt.

B_01	***Titel***
Beschreibung	*Beschreibung des gefundenen Befundes*
Auswirkung	*Nennung der möglichen Auswirkungen*
Beispiel	*[Optional] Nennung von Beispielen*
Hinweis	*[Optional] Nennung von Hinweisen*
Empfehlung	*Eine Empfehlung, was getan werden muss, damit der Befund langfristig behoben wird.*
Referenzen	*[Optional] Nennung von Referenzen*
Risikobewertung	Hoch Kritisch
Begründung	*[Optional] Nennung einer Begründung*
Behebungsstatus	*Dokumentation des Stands der Behebung*

Befunde der Kategorien „Mittel", „Niedrig", „Anmerkung" und „Verbesserung" werden wegen der geringen Priorität wie erwähnt nur überblicksartig dargestellt.

2.2.2. Risikobewertung

Die Risikobewertung von Befunden wird auf Grundlage der möglichen Folgen in folgenden Kategorien vorgenommen.

- Verbesserung:
  Der Befund erhöht das Sicherheitsniveau im Vergleich zum vorherigen Niveau. Eventuell ist jedoch noch eine zusätzliche Dokumentation im Sicherheitsregelwerk nötig.
- Anmerkung:
  Die Behebung würde das Sicherheitsniveau nicht erhöhen, dient jedoch zur Verbesserung der Darstellung oder Verständlichkeit der Dokumentation. Die Umsetzung wird angeraten, ist jedoch nicht dringend umzusetzen.
- Niedrig:
  Die Behebung würde eine Verbesserung des Sicherheitsniveaus in geringem Umfang bedeuten, dient jedoch mehr der Verbesserung der Verständlichkeit der Dokumentation. Die Umsetzung ist langfristig anzugehen.
- Mittel:
  Die Behebung würde eine Verbesserung des Sicherheitsniveaus in deutlichem Umfang bedeuten. Die Umsetzung ist mittelfristig anzugehen.
- Hoch:
  Die Behebung würde eine Verbesserung des Sicherheitsniveaus in erheblichem Umfang bedeuten. Die Umsetzung ist kurzfristig anzugehen.
- Kritisch:
  Der Befund steht einem Betrieb entgegen. Die Umsetzung ist vor einem (Weiter-)Betrieb anzugehen.

2.3. Schwachstelle

2.3.1. Darstellungsform

Folgende Darstellungsform wurde für die identifizierten Schwachstellen gewählt.

W/S_01	***Titel***
Beschreibung	*Beschreibung der gefundenen Schwachstelle*
Auswirkung	*Nennung der möglichen Auswirkungen*
Beispiel	*[Optional] Nennung von Beispielen*
Hinweis	*[Optional] Nennung von Hinweisen*
OWASP Top 10	*[Optional bei Prüfungen auf Anwendungsebene] Referenzierung der Risikokategorie aus den TOP-10-Risiken des Open Web Application Security Projects.*
Empfehlung	*Eine Empfehlung, was getan werden muss, damit die Schwachstelle langfristig behoben wird.*
Referenzen	*[Optional] Nennung von Referenzen*
Risikobewertung	None Low Medium High Critical *Errechneter Zahlenwert (CVSS3.1 Vektor-String zur Rückverfolgung der Berechnung in der Bewertung[1] und zur Weiterberechnung durch den Kunden mit z. B. dem Environmental Score)*
Behebungsstatus	*Dokumentation des Stands der Behebung*

[1] Der Vektorstring kann in folgendes URL-Schema nach dem Raute-Symbol eingetragen werden, um das Berechnungswerkzeug der FIRST zu verwenden: https://www.first.org/cvss/calculator/3.1#<VEKTOR-STRING>

2.3.2. Risikobewertung

Für Schwachstellen erfolgt eine Bewertung des Risikos nach dem Common Vulnerability Scoring System (CVSS).[2] CVSS ist der Industriestandard zur Bewertung von Schwachstellen und wurde von der Organisation FIRST (Forum of Incident Response and Security Teams) entwickelt. Aus diesem Schema ergibt sich die nachfolgende Kategorisierung, die in Tabelle 4 dargestellt ist.

Tabelle 4: Zuordnung der CVSS-Scores zu den Kategorien

CVSS-Score	CVSS-Bewertung	Zugeordnete Kategorie
0	None	Anmerkung
0,1 - 3,9	Low	Niedrig
4,0 - 6,9	Medium	Mittel
7,0 - 8,9	High	Hoch
9,0 - 10,0	Critical	Kritisch

2.4. Gemeinsame Anteile

Für die beiden Unterscheidungen „Befund“ und „Schwachstelle“ gelten allgemein einzelne Hinweise, welche in den folgenden Unterkapiteln dargestellt werden.

2.4.1. Zuordnung zu Risikostufen des alten Gutachtens

Die verwendeten Kategorien von Risiken werden den Risikostufen, die im ursprünglichen Gutachten verwendet wurden („betriebsverhindernd“, „betriebsbehindernd“ und „sonstige“), wie folgt zugeordnet:

Tabelle 5: Zuordnung der verwendeten Kategorien zu Kategorien des alten Gutachtens

Kategorie neu	Kategorie alt
Kritisch	**A – Betriebsverhindernde Schwachstelle oder Befund** Die Behebung vor Betriebsübergabe wird dringend empfohlen.
Hoch Mittel	**B – Betriebsbehindernde Schwachstelle oder Befund** Eine Behebung sobald wie möglich wird empfohlen.
Niedrig Anmerkung	**C – Sonstige/r Schwachstelle oder Befund**

[2] https://www.first.org/cvss/

Kategorie neu	Kategorie alt
Verbesserung	Lediglich unerhebliche Auswirkungen auf den Betrieb sind zu erwarten, eine Behebung wird empfohlen, soweit dies mit verhältnismäßigem (am möglichen Schaden bemessenen) Aufwand möglich ist.

2.4.2. Empfehlung

Eintragungen im Bereich der Empfehlung beschreiben beispielhafte Maßnahmen, die umgesetzt werden könnten, um den Befund oder die Schwachstelle zu beseitigen. Die Maßnahmen stellen lediglich mögliche Lösungen dar und sollen belegen, dass die Schwachstelle beseitigt werden kann. Die Notwendigkeit und Priorität der Schwachstellenbehebung hängt aber nur von der bereits beschriebenen Risikoeinstufung ab.

2.4.3. Angaben zum Status der Behebung

Der Status der Behebung gibt den Stand der Schwachstelle oder des Befundes zum Stichtag an, ob die Schwachstelle/der Befund durch den Gutachter verifiziert behoben wurde. Dabei gelten die nachfolgenden Definitionen:

- Nicht verifiziert/Nicht bearbeitet (-)
  Eine Bearbeitung der Schwachstelle oder des Befundes durch die Betreiberin liegt noch nicht vor oder es wurde noch kein erneuter Test/Begutachtung durch den Gutachter durchgeführt.
- Verifiziert: Schwachstelle/Befund behoben (J)
  Die festgestellte Schwachstelle oder der Befund konnte nicht mehr nachgewiesen werden bzw. eine adäquate Veränderung hat stattgefunden. Die Schwachstelle bzw. der Befund wird daher zum Stichtag als vollständig behoben angesehen.
- Verifiziert: Schwachstelle/Befund teilweise behoben (T)
  Eine Behandlung der Schwachstelle oder des Befundes hat stattgefunden, jedoch sind noch nicht alle Aspekte zum Stichtag behoben. Die Schwachstelle bzw. der Befund wird daher zum Stichtag als teilweise behoben angesehen.
- Verifiziert: Schwachstelle/Befund nicht behoben (N)
  Eine Behandlung der Schwachstelle oder des Befundes hat stattgefunden, jedoch ist bei einer erneuten Begutachtung die Schwachstelle oder der Befund erneut aufgefallen, oder die Behandlung wird als nicht ausreichend bewertet. Die Schwachstelle bzw. der Befund wird daher zum Stichtag als nicht behoben angesehen.

3. DOKUMENTENPRÜFUNG

3.1. Beschreibung des Analysegegenstandes

Der untersuchte Analysegegenstand bestand aus den durch die vorherige Betreiberin erstellten und von der zukünftigen Betreiberin überarbeiteten Konzeptdokumentation des beA in der vorgelegten und zum Stichtag gültigen Version.

In der Konzeptdokumentation wurden Inhalte des Sicherheitsregelwerks bestehend aus den Dokumenten

- IT-Sicherheitskonzept,
- Betriebssicherheitskonzept,
- Schlüsselmanagement und
- Kryptokonzept

tiefgehend geprüft.

Weiterhin wurden mehrere Anteile der betrieblichen Dokumentation auf relevante Zusammenhänge mit der Informationssicherheit des beA geprüft.

3.2. Methodik und Vorgehensweise

Bei der tiefgehenden Analyse des Sicherheitsregelwerks wurden die bisherige Strukturanalyse (Asset-Register), Schutzbedarfsanalyse und Risikoanalyse sowie die bisherigen allgemeinen (ISMS-Anteil) und die beA-spezifischen Sicherheitsanforderungen den jeweiligen fortgeschriebenen Anteilen, ebenso wie den Konzepten für das Schlüsselmanagement und die Kryptografie, gegenübergestellt. Hierbei aufgetretene Abweichungen wurden genauer betrachtet und bei einer Verschlechterung als Befund aufgenommen. In einem nächsten Schritt wurden die so gefundenen Befunde entsprechend den beschriebenen Risikobewertungen klassifiziert.

Zusätzlich wurden die weiteren Konzeptdokumente sowohl nach zusätzlichen neuen Sicherheitsfunktionen wie auch nach potenziellen, nicht betrachteten Risiken untersucht. Die gefundenen Sicherheitsfunktionen wurden in Eintragungen gegenüber der neuen Betreiberin und der BRAK vermerkt, um im Rahmen der weiteren Fortschreibung adressiert werden zu können. Die gefundenen Risiken wurden aufgenommen und im Audit hinterfragt.

3.3. Übersicht der Befunde

Tabelle 6: Übersicht der Befunde bei der Dokumentenprüfung

Dokument	Befund	Bewertung	behoben
Betriebssicherheits-konzept	B_01 Vollständigkeit des Asset-Registers erscheint nicht gegeben	Hoch	-
Betriebssicherheits-konzept	B_02 Rechtetrennung und -konzept/Identitätsmanagement unzureichend	Hoch	J
Betriebssicherheits-konzept & IT-Sicherheits-konzept	B_03 Mehrfaktorauthentifizierung administrativer Zugriffe entfernt	Hoch	T

Dokument	Befund	Bewertung	behoben
Betriebssicherheits-konzept	B_04 Passwortregelung nur zum Teil nach neuer BSI-Empfehlung angepasst	Hoch	T
Betriebssicherheits-konzept	B_05 Zonenkonzept nicht mehr umgesetzt	Hoch	J
Betriebssicherheits-konzept	B_06 Entwicklungsumgebung unzureichend dokumentiert	Hoch	J
Sicherheits-regelwerk	B_07 Stellenweise fehlende Dokumentation (transitionsbedingt)	Mittel	-
Betriebssicherheits-konzept & IT-Sicherheits-konzept	B_08 Fehlender Bezug der Controls des Betriebssicherheitskonzeptes im IT-Sicherheitskonzept	Mittel	-
Security Incident	B_09 Ereigniskategorie „Datenschutzvorfall“ nicht explizit im Incident Management erwähnt	Mittel	J
Betriebskonzept	B_10 Datensicherung mit Georedundanz	Verbesserung	-
Betriebskonzept	B_11 Mehrfach gestuftes Verfahren für Updates für die eingesetzte Hardware	Verbesserung	-

Bei der Prüfung der Dokumente „Kryptokonzept“ und „Schlüsselmanagement“ konnten aus Sicht des Prüfers Befunde und Verbesserungspotenziale festgestellt werden, die sich auf die Struktur der Dokumente, die Dokumentation der Prozesse und mögliche Klarstellungen bezogen. Hieraus konnten allerdings keine Schwächen der Prozesse selbst abgeleitet werden.

Die Befunde werden nachfolgend nicht aufgelistet oder festgehalten, da sie nicht Teil des eigentlichen Prüfgegenstandes waren. Der Ursprung der Befunde liegt nicht in der Fortschreibung, und somit lassen sich diese nicht der neuen Betreiberin zuschreiben.

3.4. Beschreibung der Befunde

3.4.1. Befunde der Kategorie Kritisch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „kritisch“ identifiziert werden.

3.4.2. Befunde der Kategorie Hoch

B_01 Vollständigkeit des Asset-Registers erscheint nicht gegeben

Beschreibung: Die Vollständigkeit des Asset-Registers erscheint nicht gegeben. Zum Beispiel sollten auch externe Systeme und Dienstleistungen dazu gehören. Dies ist und war auch davor nicht der Fall.

	Zusätzlich sollten die Assets mit den Objekten der Strukturanalyse des IT-Sicherheitskonzeptes übereinstimmen.
Auswirkung	Assets, die im Sicherheitsregelwerk und im Betriebskonzept nicht auftauchen, können Risiken beinhalten, die ggf. nicht behandelt werden. Die Verknüpfung des Begriffs „Asset“ mit der Strukturanalyse bietet eine methodische Brücke für die gewählte Methodik. Assets, die aus betrieblichen Gründen im Sinne einer Anwendung eingesetzt werden, fehlen aktuell ebenso, sind jedoch grundlegend für die betriebliche Umgebung von beA.
Beispiel	Aktuell fehlen zum Beispiel verwendete Backup-Services, die Entwicklungsumgebung, die Virtualisierungsumgebung sowie entsprechende Repositories.
Hinweis	Im bisherigen Sicherheitsregelwerk waren ebenso nicht alle Anteile sichtbar. Die stärkere Aufteilung der betrieblichen Anteile und Einbeziehung auch externer cloudbasierter Dienste macht die Nachführung erforderlich.
Empfehlung	Vervollständigung des Asset-Registers und Verweis auf die Strukturanalyse innerhalb des IT-Sicherheitskonzeptes.
Risikobewertung	Hoch
Begründung	Assets, die in der Strukturanalyse bzw. im Betriebskonzept nicht auftauchen, können Risiken beinhalten, die ggf. nicht behandelt werden.
Behebungsstatus	Nicht bearbeitet. Da es sich um eine methodische Erweiterung des Sicherheitsregelwerks handelt, ist mit einer längerfristigen Behebung zu rechnen. Lösungsansätze und Ideen der Umsetzung, die grundsätzlich zur Befundbehebung geeignet sind, sind durch die zukünftige Betreiberin zu erkennen und sollten im aufgebauten ISMS aufgegriffen werden.

B_02 Rechtetrennung und -konzept/Identitätsmanagement unzureichend

Beschreibung	Das bisher dokumentierte Rechte- und Rollenkonzept ist zu grob. Es enthält keine unterschiedlichen Rechte und nur sehr wenige Rollen. Auch ist die technische Umsetzung nur begrenzt vorhanden.
Auswirkung	Ein fehlendes Rechtekonzept kann zu falsch vergebenen Rechten führen. Diese können missbräuchlich genutzt werden und zu einem hohen Schaden führen.
Empfehlung	Es sollte eine genaue Dokumentation darüber erstellt werden, welche Rolle (Organisationen/Teams und Aufgaben) auf welchen Systemen über welche Authentifizierungs-Domäne welche Rechte haben. Ebenso sollte ein Konzept erstellt werden, welche Rollen für die Vergabe und Entziehung von Rechten verantwortlich sind und welchen Prozessen gefolgt werden muss. Hierbei sollte auch eine regelmäßige Prüfung enthalten sein. Nach der Dokumentation sollte dieses Konzept entsprechend auch technisch umgesetzt werden.
Risikobewertung	Hoch
Behebungsstatus	Befund wurde behoben und durch die Prüfer verifiziert.

Eine Dokumentation des Rechte- und Rollenkonzeptes wurde im Sicherheitsregelwerk erstellt.

B_03 Mehrfaktorauthentifizierung administrativer Zugriffe entfernt

Beschreibung	Die bisherige beA-spezifische Sicherheitsmaßnahme der Mehrfaktorauthentifizierung bei administrativen Zugriffen ist nicht mehr dokumentiert. Es muss davon ausgegangen werden, dass diese daher auch nicht mehr umgesetzt ist.
Auswirkung	Durch den Wegfall der Mehrfaktorauthentifizierung ist es Angreifern leichter möglich, in die Systeme einzudringen. Der spezifische Schutz der beA-Umgebung im Rahmen eines Betriebs in Rechenzentrums-Strukturen, die von mehreren Kundenkreisen genutzt werden, ist schwächer, weil eine Sicherheitsstufe fehlt.
Empfehlung	Implementierung und Dokumentation einer gleichwertigen Maßnahme. Ggf. sollte auch für die Transitionsphase der Übergang beschrieben werden.
Risikobewertung	Hoch
Behebungsstatus	Befund wurde teilweise behoben und durch die Prüfer verifiziert. Im Vor-Ort-Audit wurde erläutert, dass für einen Teil der zukünftigen Betreiberin der Zugriff auf die Systeme nur über zwei getrennte Authentifizierungs-Domänen möglich ist. Dies wird für den anderen Teil zeitnah angestrebt. Hierzu wird ein betriebliches Identitätsmanagement, das ausschließlich für die beA-Komponenten zuständig ist, umgehend angebunden. Dies dient als eine Authentifizierungs-Domäne. Die Lösung mit zwei getrennten Authentifizierungs-Domänen wird als gleichwertiger Schutz betrachtet. Die Dokumentation ist im Sicherheitsregelwerk schon erfolgt. Es ist ein Zeitplan für die weitere zeitnahe Umsetzung definiert.

B_04 Passwortregelung nur zum Teil nach neuer BSI-Empfehlung angepasst

Beschreibung	Die Änderung der Empfehlungen des BSI zum zyklischen Passwortwechsel wurde im Rahmen der Fortschreibung schon eingearbeitet. Jedoch wurde hierbei der Zusatz des BSI, dass ohne zyklischen Passwortwechsel ein starkes Passwort verwendet werden sollte, sowie eine Kompromittierung für den Nutzer erkennbar sein muss, nicht beachtet.
Auswirkung	Kurze Passwörter könnten kritisch sein, wenn diese nicht mehr zwingend geändert werden. Sollte eine Kompromittierung vorliegen, kann diese lange ausgenutzt werden, wenn das Passwort nicht mehr geändert wird.
Empfehlung	Anpassung und Ausführung von Kerninhalten der Passwortrichtlinien im Betriebssicherheitskonzept.
Referenzen	BSI-Grundschutz ORP.4.A22 und A23
Risikobewertung	Hoch

Behebungsstatus	Befund wurde teilweise behoben und durch die Prüfer verifiziert. Die Behebung ist im Zusammenhang mit der Einbindung des betrieblichen Identitätsmanagements zu sehen. In diesem erfolgt eine Umsetzung von technischen Anteilen. Da jedoch nicht alle Anforderungen technisch gelöst werden können, sind organisatorische Richtlinien erstellt worden.

B_05 Zonenkonzept nicht mehr umgesetzt

Beschreibung	Die Netzwerktrennung durch die Umsetzung eines Zonenkonzeptes ist nicht mehr dokumentiert. Dies gilt ebenso für virtuelle Netzstrukturen. Es muss davon ausgegangen werden, dass die Sicherheitsmaßnahme der strikten Netztrennung nicht mehr umgesetzt ist.
Auswirkung	Eine Netztrennung erschwert es einem Angreifer, Zugriff auf die Daten und Systeme der entsprechenden Umgebung zu erhalten. Somit verringert eine fehlende Netztrennung das Sicherheitsniveau der betriebenen Umgebung und erleichtert es Angreifern beispielsweise, Informationen offenzulegen.
Empfehlung	Erläuterungen der technischen Maßnahmen und grundlegende Überlegungen zur Netztrennung sollten im Betriebssicherheitskonzept ausgeführt oder Richtlinien anderweitig transparent gemacht werden.
Risikobewertung	Hoch
Behebungsstatus	Befund wurde behoben und durch die Prüfer verifiziert. Im Vor-Ort-Audit wurden die im Einsatz befindlichen VLANs nachvollziehbar erläutert. Im Nachgang wurde eine Dokumentation mit den Überlegungen, die hinter dem Konzept stehen, im Sicherheitsregelwerk erstellt. Die Kommunikation zwischen den VLANs wird geeignet kontrolliert.

B_06 Entwicklungsumgebung unzureichend dokumentiert

Beschreibung	An einigen Stellen des geprüften Sicherheitsregelwerks und der Betriebsdokumentation konnte erkannt werden, dass sich die Entwicklungsumgebung und der Workflow von der Entwicklung zum Betrieb grundlegend geändert haben. Diese Änderung ist nicht im Betriebssicherheitskonzept dokumentiert.
Auswirkung	Schwachstellen in der Entwicklungsumgebung und der Entwicklungsphase sowie bei der Übergabe an die Betriebsabteilung könnten übersehen werden.
Empfehlung	Die Beschreibung der tatsächlichen Struktur und Abläufe sollte vorgenommen werden. Das Thema überspannt mehrere Bereiche im Sicherheitsregelwerk und sollte deshalb grundlegend angegangen werden.
Risikobewertung	Hoch
Behebungsstatus	Befund wurde behoben und durch die Prüfer verifiziert. Im Vor-Ort-Audit konnte durch Aussagen der neuen Betreiberin belegt werden, dass das Sicherheitsniveau der Entwicklung vergleichbar mit dem

Ausgangsniveau ist. Dies wurde anschließend im Sicherheitsregelwerk noch dokumentiert.

3.4.3. Befunde der Kategorie Mittel

In der Dokumentenprüfung fiel eine aktuell bestehende Dokumentationsschwäche (vgl. B_07) der beiden Unternehmen auf. Diese hängt mit der Transitionsphase und dem gleichzeitig noch im Aufbau befindlichen ISMS mit den formalen und auf Nachweisen und Dokumenten basierenden Anforderungen zusammen. Es musste jedoch festgestellt werden, dass auch im bisherigen Sicherheitsregelwerk an vielen Stellen eine teilweise recht generische und wenig konkrete Ausführung und Darstellung gegeben war. Mit den jetzt gegebenen Feststellungen und den schon begonnenen Arbeiten für ein zertifiziertes ISMS in Form von ersten Ausarbeitungen und einem konkreten Zeitplan, ist eine langfristige Verbesserung der Sicherheit zu erwarten. Der Zeitplan sieht hierbei für beide beteiligte Unternehmen der Betreiberin den Abschluss der Zertifizierung des ISMS spätestens im ersten Halbjahr 2021 vor.

Zusätzlich wurden kleinere Auffälligkeiten gefunden, wie ein entfernter Bezug der Controls des Betriebssicherheitskonzeptes im IT-Sicherheitskonzept (vgl. B_08) oder dass eine Ereigniskategorie „Datenschutzvorfall“ nicht explizit im Incident Management erwähnt wurde (vgl. B_09).

Der entfernte Bezug wird im Nachgang der Transition korrigiert und die Konkretisierung der Definition von „Incidents“ wurde schon im Betriebsmanagementkonzept durchgeführt.

Die Befunde der Kategorie „Mittel“ und darunter wurden direkt in der bestehenden elektronischen Dokumentenbasis für das Sicherheitsregelwerk vermerkt, sodass eine zielgerichtete Behebung möglich ist.

3.4.4. Befunde der Kategorie Niedrig

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „Niedrig“ identifiziert werden.

3.4.5. Anmerkungen

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „Anmerkung“ identifiziert werden.

3.4.6. Verbesserungen

Bei der Dokumentenprüfung wurden auch Verbesserungen des Sicherheitsniveaus im Vergleich zum Ausgangsstand festgestellt.

So wird durch eine regelmäßige Kopie der Datenbank in ein an einem entfernten Standort angemietetes Rechenzentrum eine zusätzliche Georedundanz (vgl. B_10) erzeugt. Das Rechenzentrum weist ebenso ein entsprechendes Sicherheitsniveau auf.

Auch führt die Rockstein AG ein mehrfach gestuftes Verfahren für Updates für die eingesetzte Hardware (vgl. B_11) durch, in dem sie Updates der Systeme zuerst in eigene Systeme gleichen Modells einspielt und testet. Erst nach erfolgreichen Tests werden Updates in die beA-Testumgebung und zum Schluss in die beA-Produktivumgebung eingespielt.

4. UMSETZUNGPRÜFUNG DURCH AUDIT UND KONFIGURATIONS-PRÜFUNG

4.1. Beschreibung des Analysegegenstandes

Im Rahmen des geplanten Betriebsübergangs an die neue Betreiberin wird die der beA-Anwendung zu Grunde liegende Technik an einigen Stellen verändert. Zusätzlich sind die allgemeinen Sicherheitsanforderungen sehr stark an die Betriebsabläufe des zuständigen Betreibers gebunden. Beide Änderungen machten eine Überprüfung der Umsetzung der allgemeinen und spezifischen Sicherheitsanforderungen aus dem Sicherheitsregelwerk bei der zukünftigen Betreiberin notwendig.

Bei der Umsetzungsüberprüfung erfolgte daher eine anteilige Kurzrevision der allgemeinen Sicherheitsanforderungen entlang grundlegender Betriebsabläufe, eine Überprüfung der beA-spezifischen Sicherheitsanforderungen und eine Konfigurationsprüfung für Komponenten.

Hierzu wurden überwiegend die Erkenntnisse aus der Dokumentenprüfung herangezogen. Ebenso konnten durch das Vor-Ort-Audit schon einige Befunde der Dokumentenprüfung geklärt werden (siehe hierzu den Status der Behebung bei Befunden der Dokumentenprüfung).

Die grundlegenden Betriebsabläufe, die hierbei betrachtet wurden, sind

- die Administration,
- der Betrieb der Komponenten,
- die Entwicklung und
- die Übergabe von Entwicklung an den Betrieb.

Die beA-spezifischen Sicherheitsanforderungen umfassten überwiegend die Administration der HSMs und der Schutz der Integrität der beA Client Security.

Die Konfigurationsprüfung bezog sich insbesondere auf die Komponenten und IT-Systeme der beA-Anwendung, die durch den Betriebsübergang geändert wurden.

4.2. Methodik und Vorgehensweise

Diese Überprüfung erfolgte in Form eines Vor-Ort-Audits und einer Konfigurationsprüfung bei der zukünftigen Betreiberin.

Hierbei wurden in mehreren Interviewrunden der Stand der Umsetzung geprüft und durch Inaugenscheinnahme des Rechenzentrums sowie mancher Konfigurationen der Komponenten und IT-Systeme eine Verifizierung der Aussagen durchgeführt.

4.3. Übersicht der Befunde

Tabelle 7: Übersicht der Befunde bei der Umsetzungsprüfung

Anteil	Befund	Bewertung	behoben
Allgemeine Sicherheitsanforderungen	B_12 Änderungen in internen und daher projektübergreifenden Richtlinien und Vorgaben für Auftraggeber nicht erkennbar	Mittel	-
Allgemeine Sicherheitsanforderungen	B_13 Fehlende Restore-Übung der Oracle DB	Mittel	J

Anteil	Befund	Bewertung	behoben
Allgemeine Sicherheitsanforderungen	B_14 keine Schwellwerte für system- oder anwendungsbedingte Fehlermeldungen	Mittel	T
Spezifische Sicherheitsanforderungen	B_15 Zusätzliche Absicherung der HSM-Administrationsoberfläche	Verbesserung	J

4.4. Beschreibung der Befunde

4.4.1. Befunde der Kategorie Kritisch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „kritisch“ identifiziert werden.

4.4.2. Befunde der Kategorie Hoch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „hoch“ identifiziert werden.

4.4.3. Befunde der Kategorie Mittel

In der Umsetzungsprüfung wurde festgestellt, dass Änderungen in internen und daher projektübergreifenden Richtlinien und Vorgaben für Auftraggeber nicht erkennbar (vgl. B_12) sind. Als Folge sind Änderungen in allgemeinen Richtlinien und Vorgaben der Betreiberin für die BRAK als Auftraggeber nicht nachvollziehbar, wenn im Sicherheitsregelwerk nur auf diese verwiesen wird.

Durch die jetzige Prüfung ist ein ausreichendes Sicherheitsniveau gegeben, das der Auftraggeber voraussetzt. Dies bezieht jedoch auch interne und projektübergreifende (also nicht beA-spezifische) Richtlinien und Vorgaben der Betreiberin mit ein.

Durch Änderungen in diesen Richtlinien und Vorgaben könnte potentiell das Sicherheitsniveau gesenkt werden, ohne dass der Auftraggeber dies mitbekommt. Ein Mechanismus, der Änderungen in verweisenden Richtlinien auch an den Auftraggeber kommuniziert, muss entwickelt werden.

Zum Zeitpunkt der Umsetzungsprüfung wurde noch keine Restore-Übung der Oracle DB (vgl. B_13) durchgeführt. Diese wurde im Nachgang durchgeführt.

Auch sind durch die neue Betreiberin noch keine Schwellwerte für system- oder anwendungsbedingte Fehlermeldungen (vgl. B_14) definiert worden. Da von der bisherigen Betreiberin keinerlei Schwellwerte übergeben wurden, müssen diese im Anlaufprozess erstellt werden. Ebenso sind die Prozesse bei Überschreiten der Grenzwerte überblicksartig im Sicherheitsregelwerk aufgenommen worden.

4.4.4. Befunde der Kategorie Niedrig

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „niedrig“ identifiziert werden.

4.4.5. Anmerkungen

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „Anmerkung“ identifiziert werden.

4.4.6. Verbesserung

Im Rahmen der Umsetzungsprüfung wurde festgestellt, dass es eine zusätzliche Absicherung der HSM-Administrationsoberfläche (vgl. B_15) gibt. Diese ist nur verfügbar, wenn aktiv Änderungen an der HSM nötig sind. Hierzu muss mit beA-spezifischen Berechtigungen der „HSM-JSS-System-Administrator“ gestartet werden, der im Regelbetrieb üblicherweise nicht hochgefahren wird.

Die automatisierte Bereitstellung von Systementitäten und die dafür verwendete Basis aus Repositories stellt eine sehr gut steuerbare und nachvollziehbare Möglichkeit für abgesicherte und gehärtete Systemumgebungen bereit. Die Beschreibung dafür ist in der betrieblichen Dokumentation enthalten.

5. EXTERNE TECHNISCHE PRÜFUNG

5.1. Beschreibung des Analysegegenstandes

Die Anwendung „besonderes Anwaltspostfach“ soll bei einem neuen Dienstleister betrieben werden. Durch den neuen Dienstleister wurde eine Umgebung äquivalent zu der beim bisherigen Dienstleister aufgebaut, um den Betrieb der Anwendung zu übernehmen.

Die secuvera (Prüfer) wurde durch die BRAK (Kunde) beauftragt, eine technische Sicherheitsanalyse der von extern erreichbaren Komponenten der neu aufgebauten Betriebsumgebung durchzuführen.

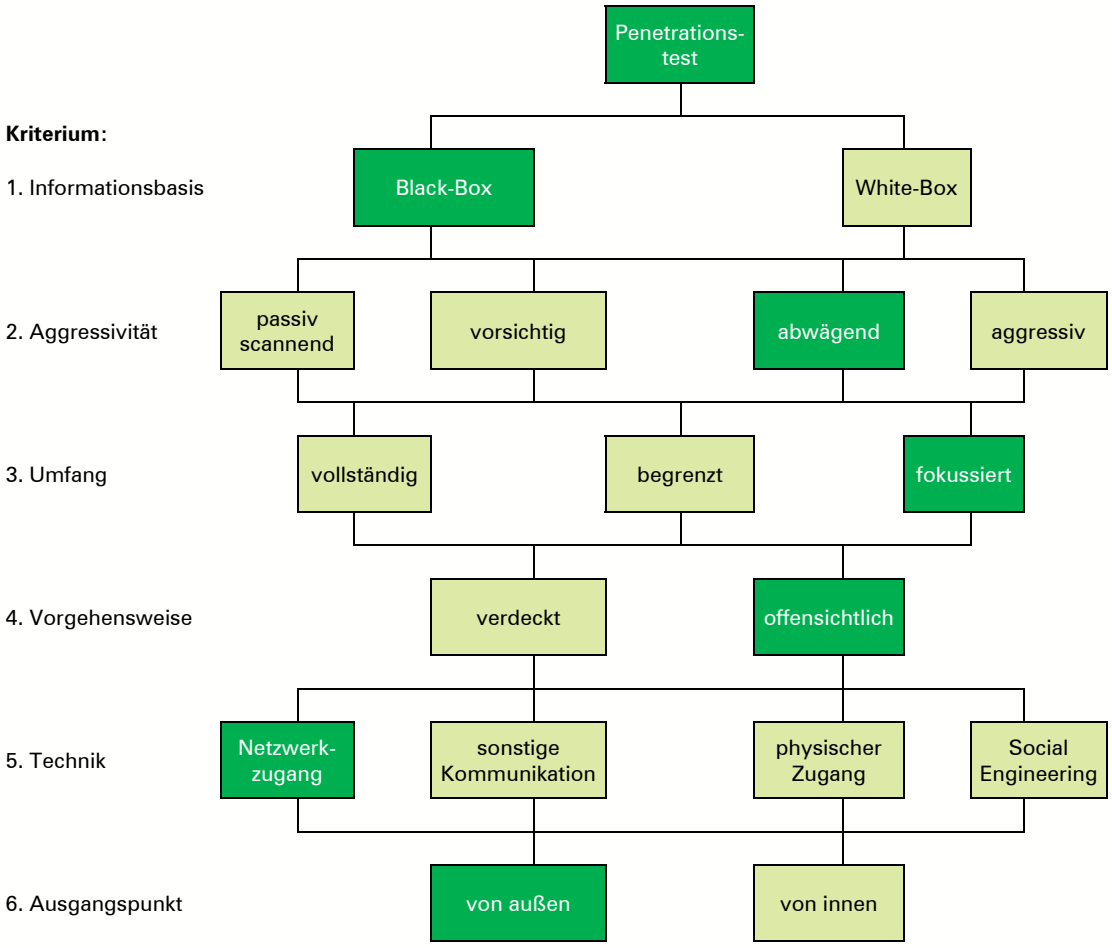
5.2. Methodik und Vorgehensweise

Vor der Prüfungsdurchführung wurden die Vorgehensweise sowie die Prüfungsgegenstände im Rahmen einer Auftaktbesprechung besprochen.

Die Prüfungen der von extern erreichbaren Anwendungsbestandteile wurden in Prüfungen auf System- und auf Anwendungsebene unterteilt durchgeführt.

Für den Penetrationstest wurde für die Prüfungen auf System- und Anwendungsebene die folgende Vorgehensweise (siehe markierte Felder) nach der BSI-Studie „Durchführungskonzept für Penetrationstests“[3] zugrunde gelegt:

Abbildung 1: Vorgehensweise nach BSI-Studie Prüfungen



[3] https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_htm.html

Sofern in einzelnen Punkten von dieser Vorgehensweise abgewichen wurde, wird dies entsprechend in der Beschreibung der Vorgehensweise erwähnt.

5.2.1. Prüfungen auf Systemebene

Durch den Dienstleister des Kunden wurden im Vorfeld der Prüfungen die extern erreichbaren IP-Adressen der beteiligten Komponenten in der Testumgebung übergeben.

Diese wurden dann im Zeitraum vom 7. bis einschließlich 11. Mai 2020 einer Sicherheitsüberprüfung in der Form eines Penetrationstests auf Systemebene unterzogen. Das Ziel dieser Prüfung war die Identifikation von technischen Schwachstellen auf Systemebene.

Die Prüfungen der Adressen wurden vollständig mit dem eigens entwickelten Framework „tajanas" durchgeführt. Tajanas basiert auf den etablierten Werkzeugen „nmap[4]" für Portscans und „OpenVAS[5]" für die Schwachstellenanalyse. Im Framework tajanas werden die Werkzeuge intelligent miteinander verknüpft und die Ergebnisse in einheitlichen Berichten aufbereitet dargestellt.

Für jede Adresse werden dabei alle 65.535 Ports TCP und aufgrund des sonst sehr hohen Zeitaufwands die „Common Ports" UDP überprüft. Ebenso wird in diesem Rahmen versucht, durch Fingerprinting die Versionen der Dienste und Betriebssysteme zu erkennen.

Hierbei werden die Dienste und Systeme so weit als möglich bezüglich folgender Eigenschaften erkannt:

- Eingesetztes Betriebssystem,
- Name der Anwendungssoftware,
- Version der Anwendungssoftware.

Wurden Dienste identifiziert, die eine Verschlüsselung der Daten auf dem Transportweg anbieten, so wurde ein Abgleich der vorliegenden Konfiguration mit den Empfehlungen der Technischen Richtlinie des Bundesamts für Sicherheit in der Informationstechnik (BSI-TR-02102) vorgenommen. Im Zuge dieses Abgleichs wird die Konfiguration auf bekannte Schwachstellen überprüft. Gefundene Schwachstellen werden dabei in theoretisch und praktisch ausnutzbar aufgeteilt.

Für die Bewertung der Ausnutzbarkeit von Schwachstellen, die als Folge einer fehlerhaften TLS-Konfiguration auftreten, wird die Annahme getroffen, dass aktuelle Clients eingesetzt werden. Als aktuelle Clients werden solche bezeichnet, bei denen alle Sicherheitsupdates (insbesondere von Browsern und TLS-Libraries), die weiter als ein Jahr zurückliegen, installiert sind. Ist eine Schwachstelle nur theoretisch oder aufgrund eines nicht aktuellen Clients ausnutzbar, so wird diese nicht explizit im Ergebnisbericht aufgeführt.

Wie vorab festgelegt, wurden keine Angriffe durchgeführt, die einen Denial-of-Service zum Ziel haben.[6]

5.2.2. Prüfungen auf Anwendungsebene

Im Zeitraum vom 7. bis einschließlich 19. Mai 2020 wurden insgesamt fünf Anwendung des Kunden einer Sicherheitsüberprüfung in der Form eines Penetrationstests durchgeführt. Das Ziel der Prüfungen war die Identifikation von Schwachstellen auf Anwendungsebene.

Die folgenden fünf Anteile der Anwendungen in der Testumgebung wurden durch den Dienstleister des Kunden übergeben:

---

[4] https://nmap.org/

[5] http://www.openvas.org/index-de.html

[6] Da die Prüfwerkzeuge in der Identifikation entsprechender Schwachstellen ohne einen DoS auszuführen sehr fehlerhaft sind, werden potentiell unzuverlässige Ergebnisse nicht aufgeführt.

Tabelle 8: Anteile der Anwendungen in der Testumgebung

Name	Applikationsversion/Datum
BRAK beA Webanwendung	2.3.5.2, Wed May 06 14:57:07 CEST 2020, bea-app-rz1-1
BRAV Suche	Nicht feststellbar
Find a lawyer (FAL, Webservice)*	1.0.7 (entnommen aus WSDL-Definition)
Zertifikatstest (Webservice)*	Nicht feststellbar
beA Safe Connector	Nicht feststellbar

Die Webanwendungen wurden ohne gültige Benutzerdaten, d. h. aus der Sicht eines anonymen Angreifers, überprüft. Durch den Kunden wurde lediglich ein X.509-Zertifikat zur Authentifizierung gegenüber dem Webserver übermittelt. Dies wurde mit dem Kunden vereinbart, um das Szenario des Verlusts der Integrität eines Zertifikats aus einer Rechtsanwaltskanzleisoftware zu betrachten. Für die beiden Anwendungen, die in Tabelle 8 mit einem Stern versehen sind, wurde das Zertifikat verwendet, da sonst eine Kommunikation auf Anwendungsebene mit den betroffenen Anwendungen nicht möglich war.

Die Anwendungen wurden zunächst mittels automatisierter Scanwerkzeuge abgetastet. Verwendet wurden hierfür die Werkzeuge „Acunetix Web Vulnerability Scanner“[7] und „Burp Suite Pro“[8]. Beide Produkte zusammen bieten derzeit erfahrungsgemäß einen hohen Abdeckungsgrad erkennbarer Schwachstellen bei automatisierten Tests. Im Anschluss daran wurden die Werkzeugergebnisse manuell verifiziert, um sog. False Positives möglichst ausschließen zu können. Die Tests wurden durch manuelle Methoden ergänzt, um prinzipbedingte Schwächen des toolgestützten Tests auszugleichen.

Bei Webservice-Schnittstellen, die eine Webservice-Definition nach der Web Service Description Language (WSDL) anboten, wurde diese mit der Burp-Suite-Pro-Erweiterung „WSDLer“[9] eingelesen, um Webservice-Aufrufe zu erstellen und diese mit dem Scanner der Burp Suite zu scannen.

Die Anwendungen werden üblicherweise von einer Webanwendungsfirewall (WAF) geschützt. Die Prüfungen wurden zunächst mit deaktivierter WAF durchgeführt. Identifizierte Schwächen wurden im Anschluss mit aktivierten Sicherheitsmechanismen erneut überprüft, um auch eine Aussage treffen zu können, inwieweit diese die Risiken der identifizierten Schwächen minimieren.

Die Tests wurden als Black-Box-Tests durchgeführt, das heißt, dass die Tester bis auf die Adresse und die Anmeldedaten der Webanwendungen keine weiteren Informationen zum technischen Aufbau und der Implementierung erhalten haben.

Als einzige Einschränkung wurde im Vorfeld der Prüfungen mit dem Kunden vereinbart, dass Prüfungen täglich an- und abzukündigen sind.

[7] http://www.acunetix.com/

[8] https://www.portswigger.net

[9] https://github.com/portswigger/wsdler

Im Rahmen der Penetrationstests der Webanwendung wurden alle technisch prüfbaren Inhalte der OWASP Top 10 (konsolidiert aus den Versionen 2004, 2007, 2010, 2013 und 2017) sowie weitere Schwachstellen geprüft.

Tabelle 9: Konsolidierte Liste der Risiken aus der OWASP Top 10

Risiko
2017 A1 – Injection
2017 A2 – Broken Authentication
2017 A3 – Sensitive Data Exposure
2017 A4 – XML External Entities (XXE)
2017 A5 – Broken Access Control
2017 A6 – Security Misconfiguration
2017 A7 – Cross Site Scripting (XSS)
2017 A8 – Insecure Deserialization
2017 A9 – Using Components with Known Vulnerabilities
2017 A10 – Insufficient Logging & Monitoring
2013 A8 – Cross Site Request Forgery (CSRF)
2013 A10 – Unvalidated Redirects and Forwards
2007 A3 – Malicious File Execution
2004 A5 – Buffer Overflow
2004 A9 – Application Denial of Service

Um eine gleichbleibende Güte der Tests und eine hohe Qualität der Prüfungen zu gewährleisten, wurde als Testgrundlage der OWASP Testing Guide in Version 4 genutzt. Auf Basis dieses Testing Guides und aufgrund von Erfahrungen aus vergangenen Penetrationstests, wurde ein speziell auf die Besonderheiten der jeweiligen Anwendung angepasster Testplan erstellt. Zusätzlich wurden weitere Analysen durchgeführt, die über die in der OWASP Top 10 benannten Risiken hinausgehen und durch den Testplan vorgegeben sind. Diese primär manuellen Untersuchungen dienen zur Prüfung der Anwendungslogik, indem dort gezielt Fehler provoziert und ausgenutzt werden sollen.

5.3. Übersicht der Schwachstellen

5.3.1. Prüfungen auf Systemebene

Tabelle 10: Zuordnung der identifizierten Schwächen zu den geprüften Systemen

Systemname	Erreichbar-keit	Schwachstellen	Risikograd Schwach-stelle	Behebungs-status	Sicherheits-niveau des Systems
Webserver beA	erreichbar	S_01 Nicht BSI-konforme SSL-/ TLS-Cipher-Suites im Einsatz	None	Siehe Schwachstel-lenbeschrei-bung	Sehr hoch
		S_02 Antwortverhalten der Firewall optimieren	None		
Schnittstellen-Anwendungs-server	erreichbar	S_01 Nicht BSI-konforme SSL-/ TLS-Cipher-Suites im Einsatz	None	Siehe Schwachstel-lenbeschrei-bung	Sehr hoch
		S_02 Antwortverhalten der Firewall optimieren	None		
Webserver Wiki	erreichbar	S_01 Nicht BSI-konforme SSL-/ TLS-Cipher-Suites im Einsatz	None	Siehe Schwachstel-lenbeschrei-bung	Sehr hoch
		S_02 Antwortverhalten der Firewall optimieren	None		
Webserver Wiki Redaktion	erreichbar	S_01 Nicht BSI-konforme SSL-/ TLS-Cipher-Suites im Einsatz	None	Siehe Schwachstel-lenbeschrei-bung	Sehr hoch
		S_02 Antwortverhalten der Firewall optimieren	None		

5.3.2. Prüfungen auf Anwendungsebene

Tabelle 11: Zuordnung der gefundenen Schwachstellen auf Anwendungsebene zu den geprüften Anwendungen

Schwachstelle	**Risikograd**	**Betroffene Webanwendungen**	**Behebungsstatus**
W_01 Verwundbare JavaScript-Bibliothek im Einsatz	Mittel	beA Web, BRAV-Suche	Behebung geplant
W_02 Fehlende HTTP-Kopfzeilen	Mittel	Alle geprüften Anwendungen	behoben

Im Folgenden wird das Ergebnis des Webanwendungspenetrationstests den in der Beschreibung der Vorgehensweise dargestellten OWASP-Top-10-Kategorien zugeordnet.

Tabelle 12: Ergebnisreferenzierung Penetrationstest auf Anwendungsebene zu OWASP-Top-10-Risiken

Risiko	beA Web	BRAV-Suche	FAL	Zertifikats-test	beA SAFE Connector
2017 A1 – Injection	Pass	Pass	Pass	Pass	Pass
2017 A2 – Broken Authentication	Pass	Pass	Pass	Pass	Pass
2017 A3 – Sensitive Data Exposure	Pass	Pass	Pass	Pass	Pass
2017 A4 – XML External Entities (XXE)	Pass	Pass	Pass	Pass	Pass
2017 A5 – Broken Access Control	Pass	Pass	Pass	Pass	Pass
2017 A6 – Security Misconfiguration	Pass	Pass	Pass	Pass	Pass
2017 A7 – Cross Site Scripting (XSS)	Pass	Pass	Pass	Pass	Pass
2017 A8 – Insecure Deserialization	Pass	Pass	Pass	Pass	Pass
2017 A9 – Using Components with Known Vulnerabilities	Fail	Fail	Pass	Pass	Pass
2017 A10 – Insufficient Logging & Monitoring	Pass	Pass	Pass	Pass	Pass
2013 A8 – Cross Site Request Forgery (CSRF)	Pass	Pass	Pass	Pass	Pass
2013 A10 – Unvalidated Redirects and Forwards	Pass	Pass	Pass	Pass	Pass
2007 A3 – Malicious File Execution	Pass	Pass	Pass	Pass	Pass
2004 A5 – Buffer Overflow	Pass	Pass	Pass	Pass	Pass
2004 A9 – Application Denial of Service	Pass	Pass	Pass	Pass	Pass

5.4. Beschreibung der Schwachstellen

5.4.1. Befunde der Kategorie Kritisch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „kritisch“ identifiziert werden.

5.4.2. Befunde der Kategorie Hoch

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „hoch“ identifiziert werden.

5.4.3. Befunde der Kategorie Mittel

W_01 Verwundbare JavaScript-Bibliothek im Einsatz

Beschreibung: Durch die Webanwendung werden JavaScript-Bibliotheken von Drittanbietern eingesetzt. Es wurden veraltete Bibliotheken identifiziert, die gegenüber bekannten Schwächen verwundbar sind. Im Abschnitt „Beispiel“ werden die identifizierten Bibliotheken aufgeführt.

Auswirkung: Durch das Ausnutzen der Schwachstellen ist ein Angreifer in der Lage, Cross-Site-Scripting-Angriffe durchzuführen, wodurch sich z. B. eigener (Schad-)Code in Anfragen platzieren ließe, der dann im Browser von potentiellen Opfern zur Ausführung kommt.

Beispiel: Folgende Versionen wurden als veraltet erkannt:

Tabelle 13: W_01 Identifizierte, veraltete Bibliotheken

Anwendungsanteil	Bibliothek	Version	Bekannte Schwachstelle(n)
beA Webanwendung	jQuery	3.4.1	CVE-2020-11022 CVE-2020-11023
BRAV Suche	jQuery	3.4.1	CVE-2020-11022 CVE-2020-11023

Hinweis: Die Informationen basieren auf Versionsinformationen. Für einen erfolgreichen Angriff gelten Randbedingungen: Die verwundbare Funktion der Bibliothek muss durch die Anwendung verwendet werden, was durch den Prüfer nicht abschließend geprüft wurde, jedoch nach Meldung des Sachverhalts durch die Anwendungsverantwortlichen verifiziert und verfolgt wurde. Ferner muss ein Opfer dazu gebracht werden, einen vom Angreifer präparierten Link anzuklicken.

OWASP Top 10: 2017 A9 – Using Components with Known Vulnerabilities

Empfehlung: Aktualisieren der jQuery-Version auf die aktuellste Version (zum Zeitpunkt der Dokumentationserstellung war dies Version 3.5.1) entsprechend dem Build-Umgebungskonzept.

Referenzen: https://blog.jquery.com/2020/05/04/jquery-3-5-1-released-fixing-a-regression/
https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6

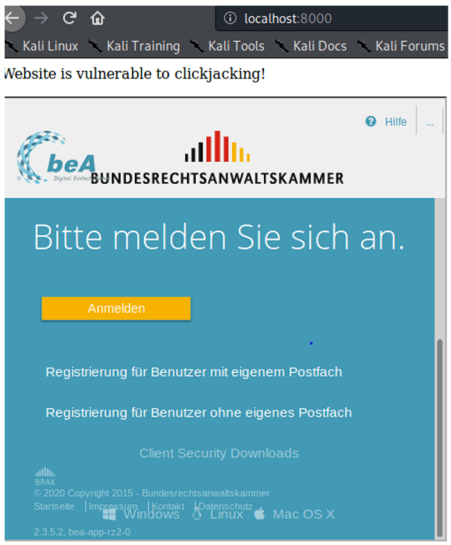
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023

Risikobewertung	Medium 4,7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N)
Behebungsstatus	Noch nicht behoben, jedoch wurde die Behebung geplant. Laut Aussage des Dienstleisters kommt die Version der Bibliothek mit der verwendeten Version des Frameworks „Primefaces“ und wird nach erfolgter Betriebsübernahme aktualisiert.

W_02 Fehlende HTTP-Kopfzeilen

Beschreibung	Die Anwendungen bzw. deren Webserver setzen in den Antwortkopfzeilen einige Header nicht, die (zusätzlichen) Schutz vor Angriffen bieten würden, da diese Sicherheitsmechanismen im Browser aktivieren. Im Rahmen der Prüfung wurde festgestellt, dass die Anwendung gegen Clickjacking-Angriffe verwundbar ist. Dem kann durch Setzen des `X-Frame-Options`-Header begegnet werden. Durch Setzen des Headers `Referrer-Policy` kann eine Weiterleitung potentiell sensibler Informationen an andere Webseiten verhindert werden. Durch Setzen des Headers `Content-Security-Policy` können die Ursprünge von aktiven Inhalten eingeschränkt und das Sicherheitsniveau gesteigert werden.
Auswirkung	Allgemein führt das Fehlen dieser Header dazu, dass die entsprechenden Sicherheitsmechanismen von Browsern nicht aktiviert werden. Dies erhöht die Wahrscheinlichkeit für erfolgreiche Angriffe. Beim Clickjacking wird die Zielwebseite über einen Frame in eine präparierte Webseite eingebunden und durch andere von einem Angreifer definierte Inhalte überlagert. Der bei der Zielanwendung angemeldete Benutzer hat den Anschein, mit den sichtbaren Elementen im Vordergrund zu interagieren, löst aber Aktionen auf der ihm nicht sichtbaren Seite im Hintergrund aus. Der Angreifer ist somit in der Lage, in der Zielanwendung Aktionen mit diesen Benutzerrechten auszuführen.
Beispiel	Für Clickjacking wurde ein Proof-of-Concept (PoC) in Form einer lokalen Webseite angelegt, die die beA-Webanwendung in einen iFrame einbindet (siehe Abbildung 2).

Abbildung 2: Clickjacking auf lokaler Webseite



Hinweis Folgende Kopfzeilen, die bei korrekter Konfiguration die Sicherheit der Webanwendung erhöhen, wurden nicht gesetzt:

Tabelle 14: Fehlende HTTP-Kopfzeilen zur Erhöhung der Sicherheit der Webanwendung

Betroffene Anwendung	**Kopfzeile**	**Beschreibung**	**Vorgeschlagener Wert**
Alle geprüften	X-Frame-Options	X-Frame-Options-Header verbessern den Schutz von Webanwendungen vor Clickjacking. Beim Clickjacking wird die Zielanwendung über einen Frame in eine präparierte Webseite eingebunden und durch andere von einem Angreifer definierte Inhalte überlagert. Der Benutzer hat den Anschein, mit den sichtbaren Elementen im Vordergrund zu interagieren, löst aber Aktionen in der ihm nicht sichtbaren Anwendung im Hintergrund aus.	`X-Frame-Options: deny` oder `X-Frame-Options: sameorigin` oder `X-Frame-Options: allow-from: DOMAIN`
Alle geprüften	Referrer-Policy	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.	`Referrer-Policy: no-referrer` oder `Referrer-Policy: strict-origin` oder `Referrer-Policy: strict-origin-when-cross-origin`

OWASP Top 10 2017 A6 – Security Misconfiguration

Empfehlung	Es wird empfohlen, die oben benannten HTTP-Security-Header nach einer Prüfung der Kompatibilität zur Anwendung einzusetzen, um die Sicherheit der Webanwendung weiter zu erhöhen.
Referenzen	https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
Risikobewertung	Medium 4,2 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N)
Behebungsstatus	Befund wurde behoben und Behebung durch den Prüfer verifiziert.

5.4.4. Befunde der Kategorie Niedrig

Bei den Prüfungen konnten mit der angewandten Prüfmethodik im Testzeitraum keine Schwachstellen mit Risikograd „niedrig“ identifiziert werden.

5.4.5. Anmerkungen

S_01 Nicht BSI-konforme Cipher Suites/Verschlüsselungs-protokolle im Einsatz

Beschreibung	Es werden Cipher Suites für die verschlüsselte Kommunikation angeboten, die nicht konform zur Technischen Richtlinie TR-02102-02 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS)“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sind.
Auswirkung	In dieser Richtlinie wird empfohlen, nur die Verschlüsselungsprotokolle TLS 1.2, 1.3 und die darin als sicher geltenden Cipher Suites zu nutzen. Eine Auflistung aller empfohlenen Cipher Suites findet sich in der TR in den Kapiteln 3.3.4 für TLS 1.2 und für TLS 1.3 im Kapitel 3.4.4. Die in dieser Richtlinie gegebenen Empfehlungen für die Verwendung von TLS werden durch die durchgeführte „Konformitätsprüfung der Transport-verschlüsselung“ reflektiert. Dabei konnten Cipher Suites identifiziert werden, die aktuell nach dieser Technischen Richtlinie nicht mehr empfohlen werden.
Empfehlung	Anpassung der TLS-Konfiguration, sodass durch den Web- oder Application-Server nur die in der Richtlinie empfohlenen Protokolle und Cipher Suites angeboten werden. Möglicherweise sind Clients im Einsatz, die die Empfehlungen des BSI nicht anwenden können. Dies ist vor allem bei Geräten der Fall, die nicht auf einem aktuellen Softwarestand gehalten werden, oder Hardwarekomponenten, für die das Gleiche gilt. Durch eine Änderung der Konfiguration würde dann keine Verbindung mehr zustande kommen können. Entsprechende Prüfungen sind vor der Produktivsetzung daher notwendig.
Referenzen	https://www.secuvera.de/blog/blogserie-zur-tls-konfiguration-technische-richtlinie-tr-02102-2-des-bsi/ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2 PDF „Konformitätsprüfung der Transportverschlüsselung“ (als Dateianhang zu diesem Dokument)
Risikobewertung	None 0,0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

Behebungsstatus Noch nicht behoben.

Laut Aussage des Dienstleisters erfordert dies ein Update der Firewall-Software, das vom Hersteller noch nicht bereitgestellt wurde, jedoch sofort nach Vorliegen installiert und die nötigen Änderungen durchgeführt werden sollte.

S_02 Antwortverhalten der Firewall optimieren

Beschreibung Bei einem Portscan wurden geschlossene Ports identifiziert. Durch den Abgleich des IP-Header-Feldes „Time-to-Live“ (TTL) konnte festgestellt werden, dass die Firewall einen Port als geschlossen meldet, da ein TCP-RST-Antwortpaket auf eine Anfrage (SYN) erhalten wurde.

Ein vorgelagertes System aus dem Netz des Anbieters Rockenstein meldet aktiv einen UDP-Port als gefiltert.

Auswirkung Durch geöffnete und geschlossene Ports lassen sich Zielsysteme besser identifizieren. Dies kann zur zielgerichteteren Analyse auf Schwachstellen und zur Präzisierung weiterer Angriffe genutzt werden.

Beispiel Folgende Ports wurden aktiv als geschlossen gemeldet:

Tabelle 15: Beispiele zu Schwachstelle S_02

System	Status
beA Webserver	HTTP-Port geschlossen (RST-Paket mit gleicher TTL wie offener HTTPS-Port erhalten).
Alle geprüften Adressen	Ein UDP-Port gefiltert (Grund: ICMP-Nachricht „Port nicht erreichbar“ erhalten).

Hinweis Das Betriebssystem ließ sich nicht abschließend bestimmen, da zu viele Fingerabdrücke zutreffend waren. Daher konnte diese Information nicht für weitere Angriffe verwendet werden.

Im Rahmen eines Vor-Ort-Termins wurde das Firewall-Regelwerk in Augenschein genommen. Es wird Port 80 auf der Adresse des beA Webservers erlaubt, jedoch ist zum Prüfzeitpunkt kein Dienst auf dem internen Zielsystem aktiv gewesen. Als Rückmeldungen zum UDP-Port wurde vom verantwortlichen Ansprechpartner genannt, dass dies durch Traceroute verursacht wird und aufseiten der Firewall nicht gefiltert, sondern aktiv durch ICMP-Nachricht abgelehnt wird.

Empfehlung Die Firewall-Konfiguration sollte angepasst werden. Anfragen an geschlossene Ports oder Traceroute-Versuche sollten ignoriert und nicht beantwortet werden. Im konkreten Fall sollte das Firewall-Regelwerk für die betreffenden Adressen angepasst werden.

Referenzen -

Risikobewertung None 0,0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

Behebungsstatus Noch nicht behoben.

Derzeit benötigen laut Aussage des Dienstleisters einige Teilnehmer am ERV den Zugriff via HTTP, da diese Teilnehmer noch nicht via HTTPS auf Port 443 zugreifen können und daher die Anforderung an die BRAK besteht, dies so anzubieten. Der Aussage folgend wird dies daher erst in Zukunft behoben, sobald die Anforderung nicht mehr besteht. Dies stellt aus Prüfersicht auch insofern keine Schwäche dar, da durch den OSCI-Standard Nachrichteninhalt und Nutzungsdaten bereits verschlüsselt übertragen werden.

6. ANHANG A: VERZEICHNISSE

6.1. Abbildungsverzeichnis

6.2. Tabellenverzeichnis