



ABSCHLUSSBERICHT

Final
Stand 26. Oktober 2021
DATAPORT

HiSolutions AG © 2021

RECHTLICHE HINWEISE

© 2021 HiSolutions AG

Der Kunde/der Auftraggeber ist nur im Umfang der mit der HiSolutions AG getroffenen Vereinbarung zur Nutzung dieser Dokumentation, insbesondere auch zu deren Vervielfältigung berechtigt. Die Veröffentlichung und die Weitergabe dieser Dokumentation an Dritte, sei es ganz oder teilweise, bedarf darüber hinaus stets der schriftlichen Einwilligung der HiSolutions AG. Ohne deren Einwilligung sind Dritte nicht berechtigt, diese Dokumentation zu nutzen.

Diese Dokumentation enthält vertrauliche Informationen, insbesondere Geschäfts- und Betriebsgeheimnisse, der HiSolutions AG sowie ggf. Dritter. Diese vertraulichen Informationen sind entsprechend gekennzeichnet und unterliegen den mit dem Auftraggeber vereinbarten Geheimhaltungsverpflichtungen. Sie dürfen danach insbesondere nicht an Dritte weitergegeben oder veröffentlicht werden.

DOKUMENTEN-STATUS

Projektname

21.dataport.ikfz Audit und Pentest

Projektnummer

57070

Dokumenten-Titel

Abschlussbericht

Autor

██████████
██████████@hisolutions.com

Seiten

73

Version

Final

Verfasst am

26. Oktober 2021

VERSIONSVERLAUF

Datum	Version	Beschreibung	Bearbeiter
19.07.2021	0.1	Datensammlung	██████████
04.08.2021	0.2	Ergebnisse IS-Webcheck	██████████
16.09.2021	0.3	Ergänzung Ergebnisse KBA-Anforderungen	██████████
20.10.2021 - 25.10.2021	0.6	Ergänzungen	██████████
26.10.2021	0.9	QS	██████████
26.10.2021	1.0	Finalisierung	██████████

MANAGEMENT SUMMARY

1.1 Ziel und Umfang

Zeitraum:	19.07.2021 bis 10.09.2021
Prüfteam (HiSolutions AG):	IS-Penetrationstests: [REDACTED] IS-Webcheck: [REDACTED] IS-Kurzrevision: [REDACTED] iKfz-Audit: [REDACTED]
Untersuchungsgegenstand:	i-Kfz relevante IT-Umgebung, Dokumentation und Prozesse

Ziel der Prüfungen war es für HiSolutions, die Prüfungen nach den KBA Mindestanforderungen für die bei Dataport betriebenen Systeme durchzuführen.

Die Prüfungen bestanden aus:

- Audit der Mindestanforderungen
- Penetrationstest inkl. IS-Webcheck
- IS-Kurzrevision für nicht vom bestehenden Grundschutzzertifikat abgedeckte Bereiche

1.2 Gesamteinschätzung

Im Rahmen des Tests wurden insgesamt 22 Schwachstellen und 2 Anmerkungen identifiziert und bewertet. Daraus lässt sich das folgende Risikoprofil ableiten. Die Zahlen verweisen jeweils auf die Nummer des Befunds in diesem Bericht.

	AKUTES RISIKO (drohende Schäden)	MITTELBARES RISIKO (drohende Schäden unter bestimmten Umständen)	LATENTES RISIKO (Schäden nur in Verbindung mit weiteren Schwachstellen)
Nichtbeachtung von KBA-Vorgaben	1, 2, 3, 4, 5, 6, 7	8, 23	
Schwachstellen durch veraltete Software	2, 14	15, 16, 17	13, 18, 20
Fehlende Mandantentrennung	7, 22	23	
Unbekannte Systeme und/oder Zuständigkeiten	1, 3, 4, 22	8	
Unbefugter Abruf von Daten (Lesen)			11, 18, 24
Unbefugter Zugriff auf Daten (Ändern)		10	12
Ausfall der Anwendung	3, 4		19

Wir beurteilen die Sicherheit der geprüften Umgebung und Eignung zum i-KFZ Betrieb insgesamt als ungenügend und voraussichtlich nicht zulassungsfähig.

1.3 Wesentliche Einzelergebnisse

Die wichtigsten Befunde aus dem Test waren:

- Das Gesamtsystem wurde aufgebaut, ohne Vorgaben des KBA zu beachten. Gegebenenfalls im Vorfeld mit dem KBA durchgeführte Absprachen konnten im Rahmen des Audits nicht belegt oder nachgewiesen werden. Entsprechend sind wesentliche Teile der Implementation wahrscheinlich nicht zulassungsfähig.
- Datenflüsse, Netzabgrenzungen, Zugriffsmöglichkeiten und Zuständigkeiten sind zum Teil unbekannt. Ein Betriebsrisiko ist dadurch nicht sinnvoll abschätzbar und die Prüfbarkeit der Umgebung erheblich erschwert.
- Das Einspielen von Sicherheitspatches sowie Wartung der Systeme sind, basierend auf einer Einschätzung der auf den Systemen vorhandenen Software-Versionsstände, verbesserungsbedürftig.

1.4 Abbildung der KBA-Anforderungen auf Befunde

Die abgeleiteten Sicherheitsanforderungen aus Kapitel 7 der "Mindest-Sicherheitsanforderungen an dezentrale Portale" des KBA bilden sich wie folgt auf Befunde ab:

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
A-6.1-1	allg.	Kommunikationswege zwischen dezentralen Portalen und dem KBA	muss	Erfüllt.
A-6.1-2	allg.	Härtung ausgewählter Komponenten	muss	Nein - An vielen Stellen fehlerhaft <i>Befunde 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, , 21</i>
A-6.1-3	allg.	Organisatorische Sicherheit	muss	Nicht geprüft im Systemaudit / Pentest Nein - Fehlende Übersicht über Systeme & Netze 3 H – Unvollständige interne Übersicht über i-Kfz Komponenten, 4 H – Mangelhafte zentrale Übersicht über notwendige oder erlaubte i-Kfz-Kommunikationsverbindungen, 8 M – Zugriffsweg und Absicherung Schnittstelle D unbekannt
A-6.1-4	allg.	Fachkunde und Zuverlässigkeit des Personals	muss	Nicht geprüft im Systemaudit / Pentest

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
A-6.1-5	allg.	Räumliche Sicherheit	muss	Nicht geprüft im Systemaudit / Pentest
A-6.1-6	allg.	System- und netztechnische Sicherheit muss sichergestellt werden.	muss	<p>Nein - Netztrennung unbekannt oder fehlt</p> <p>2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung, 5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen, 8 M – Zugriffsweg und Absicherung Schnittstelle D unbekannt, 22 H – Widersprüchliche Aussagen zur Firewall-Existenz, 23 M – Fehlende Mandantentrennung, 24 M – Server wenig abgeschirmt</p>
A-6.1-7	allg.	Incident Management	muss	Nicht geprüft im Systemaudit / Pentest
A-6.1-8	allg.	Ein Informationssicherheitskonzept muss erstellt werden.	muss	Nicht geprüft im Systemaudit / Pentest
A-6.1-9	allg.	Kommunikation zwischen den Komponenten	Muss	<p>Nein - Kommunikationswege unbekannt oder unvollständig abgesichert</p> <p>4 H – Mangelhafte zentrale Übersicht über notwendige oder erlaubte i-Kfz-Kommunikationsverbindungen, 5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen, 7 H – Schnittstelle C mit Fremd-Administratoreingriff, 8 M – Zugriffsweg und Absicherung Schnittstelle D unbekannt, 22 H – Widersprüchliche Aussagen zur Firewall-Existenz, 24 M – Server wenig abgeschirmt</p>

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
A-6.1-10	allg.	Demilitarisierte Zonen	muss	<p>Nein - DMZen nicht nach Vorschrift umgesetzt</p> <p>5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen, 22 H – Widersprüchliche Aussagen zur Firewall-Existenz, 24 M – Server wenig abgeschirmt</p>
A-6.1-11	allg.	Mandantentrennung	muss	<p>Nein – Verwendung gemeinsamer Server und Datenbanken mit teils unbekannter Trennung</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform, 23 M – Fehlende Mandantentrennung</p>
A-6.1-12	allg.	Nutzung von externen Cloud-Diensten	muss	<p>Externe Cloud-Dienste werden nicht verwendet.</p> <p>Der interne Cloud-Dienst ist nicht geeignet aufgestellt.</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform</p>
A-6.1-13	allg.	Zugangs- und Zugriffskonzept	muss	<p>Ein Konzept wurde im Systemaudit / Pentest nicht geprüft.</p> <p>Nein – Absicherung des Administrations-Zugriffs teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform, 7 H – Schnittstelle C mit Fremd-Administratoreingriff, 8 M – Zugriffsweg und Absicherung Schnittstelle D unbekannt</p>
A-6.2.1-1	A	Die Verbindung muss mit Hilfe eines IPSec-Tunnels aufgebaut werden	muss	Erfüllt.
A-6.2.1-2	A	Die IPSec-Kommunikationsteilnehmer	muss	Unbekannt – war nicht prüfbar

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
		müssen beiderseitig authentifiziert werden		
A-6.2.1-3	A	Die Vertraulichkeit der Daten muss gewährleistet werden	muss	Unbekannt – war nicht prüfbar
A-6.2.1-4	A	Die Integrität der Daten muss gewährleistet werden	muss	Unbekannt – war nicht prüfbar
A-6.2.1-5	A	Authentifizierung des i-Kfz-WS-Clients	muss	Unbekannt – war nicht prüfbar
A-6.2.2	B	Interne Schnittstelle des KBA.	-	Interne Schnittstelle des KBA.
A-6.2.3-1	C	Verwendung der Schnittstelle C	muss	Teilweise – Schnittstelle wird verwendet, aber möglicher Zugriff durch Dritte unklar 7 H – Schnittstelle C mit Fremd-Administratoreingriff
A-6.2.3-2	C	Die Integrität und Vertraulichkeit der Daten	muss	Teilweise – Schnittstelle wird verwendet, aber möglicher Zugriff durch Dritte unklar 7 H – Schnittstelle C mit Fremd-Administratoreingriff
A-6.2.3-3	C	Die Nachvollziehbarkeit muss gewährleistet werden	muss	Teilweise – Schnittstelle wird verwendet, aber möglicher Zugriff durch Dritte unklar 7 H – Schnittstelle C mit Fremd-Administratoreingriff
A-6.2.4-1	D	Die Kommunikation zwischen Zulassungsbehörden und dem KBA darf nur über definierte Verbindungen stattfinden	muss	Teilweise – Schnittstelle wird verwendet, aber möglicher Zugriff durch Dritte unklar 7 H – Schnittstelle C mit Fremd-Administratoreingriff
A-6.2.4-2	D	Zugriff auf das Postfach an der Schnittstelle D muss authentifiziert werden	Muss	Teilweise – Schnittstelle wird verwendet, aber möglicher Zugriff durch Dritte unklar 7 H – Schnittstelle C mit Fremd-Administratoreingriff
A-6.2.5	E	Interne Schnittstelle des KBA.	-	Interne Schnittstelle des KBA.

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
A-6.2.6-1	F	Die Benutzung der Schnittstelle F	muss	Erfüllt durch Umsetzung von A-6.2.6-2
A-6.2.6-2	F	Die Integration der Schnittstelle F	Kann	Unbekannt – war nicht prüfbar
A-6.2.6-3	F	Die Nachvollziehbarkeit muss gewährleistet werden	muss	Unbekannt – war nicht prüfbar
A-6.2.7	H	Schnittstelle existiert nicht: nicht implementiert	muss	Unbekannt – war nicht prüfbar (in OSI-Plattform)
A-6.2.8-1	Xn	Die Integrität der Daten muss geschützt werden	muss	<p>Nein – Umsetzung der Schnittstellen teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform 2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung, 5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen</p>
A-6.2.8-2	Xn	Die Vertraulichkeit der zu übertragenden Daten muss zu jeder Zeit gewährleistet werden	muss	<p>Nein – Umsetzung der Schnittstellen teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform 2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung, 5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen</p>
A-6.2.8-3	Xn	Die Nachvollziehbarkeit muss gewährleistet werden	muss	<p>Nein – Umsetzung der Schnittstellen teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform</p>

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
				<p>2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung,</p> <p>5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche,</p> <p>6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen</p>
A-6.2.8-4	Xn	Sichere Anbindung der lokalen Netze an das Internet	muss	<p>Nein – Umsetzung der Schnittstellen teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform</p> <p>2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung,</p> <p>5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche,</p> <p>6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen</p>
A-6.2.9-1	Yn	Die Integrität der Daten muss geschützt werden	muss	<p>Nein – Umsetzung der Schnittstellen teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform</p> <p>2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung,</p> <p>5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche,</p> <p>6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen</p>
A-6.2.9-2	Yn	Die Vertraulichkeit der zu übertragenden Daten muss zu jeder Zeit gewährleistet werden	muss	<p>Nein – Umsetzung der Schnittstellen teilweise unbekannt</p> <p>1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform</p> <p>2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der</p>

Anf.	Schnittstelle	Titel	muss?	erfüllt? (wenn nein: Befunde)
				Umgebung, 5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen
A-6.2.9-3	Yn	Die Nachvollziehbarkeit muss gewährleistet werden	muss	Nein – Umsetzung der Schnittstellen teilweise unbekannt 1 H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform 2 H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung, 5 H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche, 6 H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen
A-6.2.10+11	Xi+Yi	Absicherung der Schnittstellen Xi + Yi	muss	Nein - Schnittstellen wurden nicht implementiert

INHALTSVERZEICHNIS	
RECHTLICHE HINWEISE	I
DOKUMENTEN-STATUS	I
VERSIONSVERLAUF	I
MANAGEMENT SUMMARY	II
1.1 Ziel und Umfang	II
1.2 Gesamteinschätzung	II
1.3 Wesentliche Einzelergebnisse	III
1.4 Abbildung der KBA-Anforderungen auf Befunde	III
2 ÜBERBLICK ÜBER DIE DURCHGEFÜHRTEN TESTS	12
2.1 Kontext	12
2.2 Informationsbasis IS-Penetrationstest	13
2.3 Beteiligte Personen	13
2.4 Durchgeführte Tests	13
2.5 Hinweise zu den Ergebnissen	13
2.5.1 Bewertung der Befunde	13
2.5.2 Entscheidungsmatrix	14
2.6 Zu löschende oder zu beachtende Testrückstände	15
3 ERGEBNISSE DER IS-KURZREVISION	16
3.1 Vorgehen IS-Kurzrevision	16
3.2 Ergebnisse	16
4 AUDITIERUNG DER KBA-MINDESTANFORDERUNGEN	17
4.1 Einschränkungen	18
4.2 Ergebnisse	18
5 ERGEBNISSE DES EXTERNEN PENETRATIONSTESTS	30
5.1 Getestete Systeme und Netzbereiche	30
5.2 Vorgehen	30
5.3 Verwendete Werkzeuge	30
5.4 Ergebnisse	30
6 PRÜFUNG DER WEBANWENDUNGEN – IS-WEBCHECK	32
6.1 Getestete Seiten	32
6.2 Einschränkungen	32
6.3 Vorgehen	32
6.4 Verwendete Werkzeuge	34
6.5 Ergebnisse	34
7 INTERNER PENETRATIONSTEST	45

7.1	Getestete Systeme und Netzbereiche	45
7.2	Einschränkungen	46
7.3	Vorgehen	46
7.4	Verwendete Werkzeuge	47
7.5	Ergebnisse	47
8	KONFIG-AUDIT FIREWALLS	56
8.1	Geprüfte Firewallkonfigurationen	56
8.2	Einschränkungen	56
8.3	Vorgehen	56
8.4	Ergebnisse	56
ANHANG A BERÜCKSICHTIGUNG DER OWASP TOP TEN		61
A.1	Fehlerklassen	64
ANHANG B EMPFEHLUNGEN ZU HÄUFIGEN FEHLERKLASSEN		65
B.1	Cross-Site-Scripting (XSS)	65
B.1.1	Durchgängige Implementierung einer Ausgabecodierung	65
B.1.2	Einschränkung der Auswirkungen von XSS	66
B.1.3	Implementierung einer Eingabevalidierung auf Serverseite	66
B.1.4	Content Security Policy	67
B.2	Patch-Management	67
ANHANG C BEWERTUNGSSKALEN FÜR SCHWACHSTELLEN		69
ANHANG D SCHWACHSTELLENVERZEICHNIS		71
KONTAKT		72

2 ÜBERBLICK ÜBER DIE DURCHGEFÜHRTEN TESTS

2.1 Kontext

Dataport betreibt für Zulassungsstellen in Hamburg und Schleswig-Holstein das dezentrale Portal für die internetbasierte Fahrzeugzulassung (i-Kfz). Für den Landesbetrieb Verkehr Hamburg, den Kreis Dithmarschen und die Landeshauptstadt Kiel wird darüber hinaus auch das Fachverfahren und das am Zulassungsprozess beteiligte Verfahren Wunschkennzeichen betrieben. Weitere 13 Zulassungsstellen betreiben das Fachverfahren und die am Zulassungsprozess beteiligten Verfahren selbst.

Wo möglich und aus Sicht der Prüfer sinnvoll wurde bei der Prüfung auf Synergie-Effekte zwischen den Mandanten-Installationen zurückgegriffen.

Für drei Kunden betreibt Dataport alle Komponenten der i-Kfz-Architektur, dafür sind die Anforderungen in Kapitel 8.1 der KBA-MSADP beschrieben. Demnach sind die folgenden Prüfungen in zweijährigem Rhythmus durchzuführen:

	<i>IS-Kurzrevision¹⁰</i>	<i>IS-Webcheck</i>	<i>Penetrationstest</i>
<i>Dezentrales Portal</i>	Ja	Ja	Ja
<i>Systeme des Fachverfahrens</i>	Ja	Ja	Ja
<i>Indirekt am Zulassungsprozess beteiligte Verfahren</i>	Ja	Ja	Ja

Abbildung 1: Laut KBA für Hamburg, Dithmarschen und Kiel durchzuführende Prüfungen

Für weitere Kunden wird nur das dezentrale Portal betrieben, daher sind nur die Anforderungen aus Kapitel 8.2 der KBA-MSADP zu prüfen:

	<i>IS-Kurzrevision¹¹</i>	<i>IS-Webcheck</i>	<i>Penetrationstest</i>
<i>Dezentrales Portal</i>	Ja	Ja	Ja
<i>Systeme des Fachverfahrens</i>	Nein	Nein	Nein
<i>Indirekt am Zulassungsprozess beteiligte Verfahren</i>	Nein	Nein	Nein

Abbildung 2: Laut KBA für die übrigen Kunden durchzuführende Prüfungen

Die IS-Kurzrevision ist immer durchzuführen, wenn keine Zertifizierung nach ISO 27001 oder IT-Grundschutz vorliegt. Das Rechenzentrum und die Basisdienste sind zertifiziert, nicht jedoch das Portal und die Fachverfahren.

2.2 Informationsbasis IS-Penetrationstest

Die Tests wurden als „White-Box-Test“ durchgeführt, d. h. die Prüfer hatten, soweit vorhanden, alle notwendigen Informationen zu der zu prüfenden Umgebung.

2.3 Beteiligte Personen

An der Testdurchführung waren hauptsächlich die folgenden Personen beteiligt:

Tabelle 1: Beteiligte Personen

Ansprechpartner beim Auftraggeber

██████████
██████████

Prüfteam HiSolutions

████████████████████
████████████████████
████████████████████
████████████████████
████████████████████

Zusätzliche fachliche Ansprechpartner wurden auf Anfrage und Notwendigkeit für einzelne Themengebiete hinzugezogen.

2.4 Durchgeführte Tests

Im Rahmen des Projektes wurden die folgenden Arten von Tests durchgeführt. Eine ausführliche Darstellung des Testablaufs und der Ergebnisse finden sich in den entsprechenden Kapiteln.

- IS-Kurzrevison
- Externer Penetrationstest
- IS-Webcheck
- IS-Penetrationstest
- Konfigurations-Audit Firewalls
- KBA MSADP-Audit

2.5 Hinweise zu den Ergebnissen

Trotz der Nutzung moderner und umfassender Methoden und Werkzeuge kann eine IT-Struktur niemals zu 100 % auf Sicherheit getestet werden. Aus diesem Grund stellt dieser Bericht keine Garantie für vollständige Sicherheit dar.

Der Bericht spiegelt eine Momentaufnahme des Sicherheitsstatus wider. Dabei können folgende, sich auf den aktuellen Sicherheitsstatus auswirkende Aspekte nicht miteinbezogen werden:

- Konfigurationsänderungen nach Testende oder zwischen zeitlich getrennten Tests,
- zum Testzeitpunkt nicht verfügbare Systeme,
- Systeme, die aus dem Audit ausgeklammert worden sind, und
- nach dem Test bekannt gewordene Risiken.

2.5.1 Bewertung der Befunde

Alle Befunde wurden in eine der folgenden Kategorien eingestuft:

Tabelle 2: Bewertungskategorien

Schweregrad	Bezeichnung	Beschreibung
(C) CRITICAL	Kritische Schwachstelle	Das gefundene Problem erfordert sofortiges Handeln. Eine Information über die Schwachstelle erfolgt bereits während der Testdurchführung. Für die Schwachstelle existiert eine korrespondierende Bedrohung, die die Sicherheit des Untersuchungsgegenstandes akut gefährdet.
(H) HIGH	Schwerwiegende Schwachstelle	Das gefundene Problem erfordert kurzfristiges Handeln. Für die Schwachstelle existiert eine korrespondierende Bedrohung, die die Sicherheit des Untersuchungsgegenstandes ernsthaft gefährden kann.
(M) MEDIUM	Mittlere Schwachstelle	Das gefundene Problem erfordert mittelfristiges Handeln. Für die Schwachstelle existiert eine korrespondierende Bedrohung, die die IT-Sicherheit des Untersuchungsgegenstandes unter bestimmten Umständen gefährden kann. Eine Eskalation zu einem schwerwiegenden Problem ist möglich.
(L) LOW	Geringfügige Schwachstelle	Das gefundene Problem kann nachrangig behandelt werden, da kein entsprechendes Bedrohungsszenario erkennbar ist. Zur Steigerung der Sicherheit und zur Verhinderung zukünftiger Probleme, z. B. in Verbindung mit anderen Schwachstellen, wird eine Behebung jedoch empfohlen.
(I) INFO	Information	Der gefundene Sachverhalt stellt kein Sicherheitsrisiko dar, sondern erläutert Erkenntnisse aus dem Test, die keinen Sicherheitsbezug haben, aber für den Auftraggeber dennoch von Interesse sein können (z. B. fehlende Funktionalität).

2.5.2 Entscheidungsmatrix

Der Schweregrad ergibt sich aus den Faktoren „Komplexität des Angriffs“ und „Potenzieller Schaden“. Der Schweregrad ist dabei umso höher, je einfacher ein Schaden einzutreten droht (Komplexität des Angriffs) und je größer die potenziellen Folgen des Eintretens sind. Für beide Dimensionen werden dreistufige Skalen verwendet, die im Anhang unter *Anhang C Bewertungsskalen für Schwachstellen* näher erläutert sind.

Tabelle 3: Entscheidungsmatrix für die Bewertung

		Komplexität des Angriffs		
		<i>Elaborate</i>	<i>Complex</i>	<i>Simple</i>
Potenzielle Auswirkungen	<i>Grave</i>	MEDIUM	HIGH	CRITICAL
	<i>Serious</i>	LOW	MEDIUM	HIGH
	<i>Light</i>	LOW	LOW	MEDIUM

2.6 Zu löschende oder zu beachtende Testrückstände

Im Rahmen des Tests sind verschiedene Testdaten auf den getesteten Systemen hinterlassen worden, die von Seiten der Tester nicht vollständig beseitigt werden konnten, da beispielsweise entsprechende Berechtigungen fehlten oder sie vielleicht bereits in nicht erreichbare Backendsysteme weitergeleitet wurden.

Es wird empfohlen, die entsprechenden Daten mit der gegebenen Vorsicht zu entfernen, da insbesondere Eingaben in Webdienste oft Sonderzeichen enthalten, die für Verarbeitungsprobleme sorgen könnten.

Insbesondere sollten folgende Daten behandelt werden:

- neu angelegte Nutzerkennungen pt-████████@hisolutions.com für Mandanten SH und HH
- testweise über die dezentralen Portale SH und HH ausgelöste iKfz-Vorgänge im Prüfzeitraum (02.08.2021 bis 03.08.2021)

3 ERGEBNISSE DER IS-KURZREVISION

3.1 Vorgehen IS-Kurzrevision

Die IS-Kurzrevision verschafft dem IS-Management einen Überblick über den Sicherheitsstatus in der Institution. Betrachtet werden Aspekte aus dem IT-Grundschatz, die eine wesentliche Grundlage für Informationssicherheit bilden und sich aufgrund von Erfahrungswerten als risikobehaftet erwiesen haben.

3.2 Ergebnisse

Die Ergebnisse finden sich in dem Dokument „Abschlussbericht IS-Kurzrevision“, welches parallel zur Verfügung gestellt wird.

4 AUDITIERUNG DER KBA-MINDESTANFORDERUNGEN

Im Rahmen des Projekts wurde die Mindestanforderungen des KBA für die betrachtete Umgebung geprüft. Dies geschah teilweise durch direkte Befragung der Ansprechpartner, durch die schriftliche Bereitstellung und Beantwortung von Fragen sowie indirekt aus den weiteren Prüfungshandlungen.

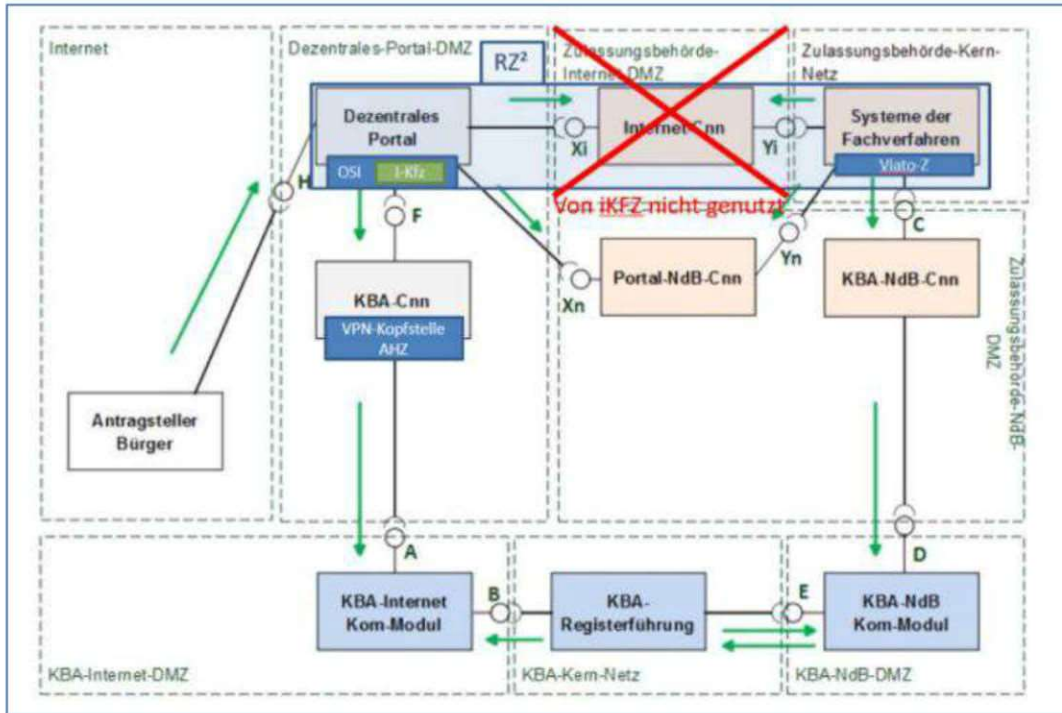


Abbildung 3: Bereitgestellter Screenshot der Referenzarchitektur.

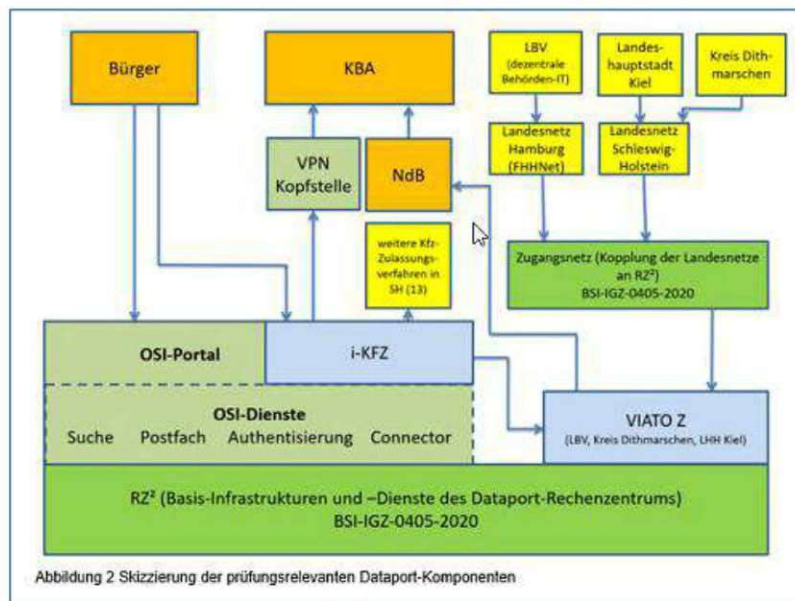


Abbildung 4: Bereitgestellter Screenshot relevanter Komponenten.

4.1 Einschränkungen

Ein Teil der Fragen konnte während des Prüfzeitraumes nicht oder nur unzureichend beantwortet werden. Es muss für diese Fragen davon ausgegangen werden, dass die Mindestanforderungen nicht erfüllt wurden, da kein entsprechender plausibler Nachweis erbracht werden konnte.

4.2 Ergebnisse

Aus der Prüfung ergaben sich folgende Befunde:

<h1 style="font-size: 48px; margin: 0;">H</h1> <p style="font-weight: bold; margin: 5px 0;">high</p>	1. H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform		Elaborate	Complex	Simple
	Fehlerklasse: Anwendung: Design-Fehler	Grave		X	
		Serious			
		Light			
Betroffene Systeme:	Übergreifender Befund (u.a. Dezentrales Portal, Systeme der Fachverfahren)				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Die i-Kfz-Anwendung des dezentralen Portals ist, zusammen mit den dazugehörigen Systemen, in eine zentrale Plattform (OSI) integriert, was einen gekapselten und nachvollziehbaren Betrieb der i-Kfz-Komponenten erheblich erschwert und schwer bis gar nicht kalkulierbaren Risiken aussetzt.</p> <p>Laut Aussage des Auftraggebers werden auf der OSI Plattform etwa 500 weitere Dienste betrieben, die ebenfalls für Bürger aus dem Internet erreichbar sind. Die darunterliegenden Serversysteme werden zwischen allen Anwendungen geteilt.</p> <p>Im Rahmen des Tests wurde durch den Auftraggeber angemerkt, dass das initiale Design bzw. die Integration der i-Kfz-Komponenten in die Plattform zuvor mit dem KBA besprochen wurde. Darüber konnten aber keine Nachweise vorgelegt werden. Der Auftraggeber wurde daraufhin gebeten, Kontakt mit dem KBA aufzunehmen und das mögliche weitere Vorgehen zu besprechen. HiSolutions konnte bis zum Projektende keine Rückmeldung erhalten, was diese Gespräche ergeben haben oder in welchem Status sich diese zu dem Zeitpunkt befanden.</p>				
Auswirkung:	<p>Die Zusammenführung der i-Kfz-Anwendung mit mehreren hundert weiteren Anwendungen des Auftraggebers erhöht die Angriffsfläche der Systeme und der verarbeiteten Daten enorm. Eine wie vorgeschrieben strikte Trennung der i-Kfz-Anwendung von anderen Anwendungen ist in der OSI-Plattform nicht gegeben.</p> <p>Dies betrifft beispielsweise auch die Webseite, wodurch Schwachstellen in anderen Teilen dieser Webseite direkte Auswirkungen auf Bürger haben, welche das dezentrale Portal verwenden wollen.</p>				

Empfehlung:	<p>Prüfen Sie, ob das initiale Design bzw. die Integration der i-Kfz-Komponenten in die Plattform zuvor mit dem KBA besprochen wurde und was das Ergebnis dieser Absprache war.</p> <p>Falls einer Einbindung damals explizit erlaubt wurde, prüfen Sie, ob die damals getätigten Aussagen zum Aufbau der Plattform weiterhin gültig sind, und ob damit ein Betrieb im aktuellen Zustand möglich ist. Prüfen Sie weiterhin, ob zusätzliche Anforderungen an den Betrieb gestellt wurden und deren Umsetzung.</p> <p>Generell entspricht der Betrieb in der aktuellen Umgebung zusammen mit den anderen Anwendungen aus Sicht von HiSolutions nicht den Anforderungen des KBA (z.B. A-6.1-6 „Die Umsetzung der Funktionalitäten des dezentralen Portals muss netztechnisch (z. B. durch Einsatz geeigneter Paketfilter) von anderen angebotenen Anwendungen des Betreibers separiert werden.“).</p>
-------------	--

<h1 style="font-size: 48px; margin: 0;">H</h1> <p style="font-weight: bold; margin: 5px 0;">high</p>	2. H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung		Elaborate	Complex	Simple
	Grave		X		
	Serious				
	Light				
Fehlerklasse: <i>Anwendung: Design-Fehler</i>					
Betroffene Systeme:	Übergreifender Befund (u.a. Dezentrales Portal, Systeme der Fachverfahren)				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Neben der Integration der i-Kfz-Anwendung in die zentrale OSI-Plattform (siehe Befund 1) existieren an diversen weiteren Stellen starke Abweichungen von den Vorgaben des KBA. So sind mehrere Schnittstellen nicht wie gefordert vorhanden (siehe Befund 6), geforderte Netzbereiche nicht vorhanden (siehe Befund 5) oder die Mandantentrennung nicht nach den Vorgaben befolgt (siehe Befund 23).</p> <p>Es war im Test nicht erkennbar, dass ein interner Prozess zur Überwachung der KBA-Mindestanforderungen existiert, durch den Änderungen der Vorgaben erkannt und behandelt werden können. Dies fiel u.a. mehrfach dadurch auf, dass nicht klar war, ob eine bestimmte Anforderung zum Zeitpunkt der Umsetzung bereits existierte oder erst in einer neueren Version hinzugekommen war.</p>				
Auswirkung:	Die aktuellen KBA-Mindestsicherheitsanforderungen an die i-Kfz-Architektur und – Systeme sind nicht strukturiert umgesetzt, teilweise inkompatibel mit großen Teilen der verwendeten Architektur und eine Anpassung daher nur schwer möglich. Ein sicherer Betrieb ist durch die Nicht-Einhaltung der Mindestanforderungen aktuell nicht wie vom KBA gefordert möglich.				
Empfehlung:	Behandeln Sie die Ergebnisse aus diesem Projekt entsprechend der jeweils getätigten Empfehlungen und führen Sie zeitnah eine proaktive Abstimmung mit dem KBA durch.				

	<p>Prüfen Sie dabei, ob eine Änderung an den bisherigen Strukturen ausreichend ist um diese kompatibel zur allgemein geforderten i-Kfz-Architektur zu machen, oder ob ein Neu-Aufbau, der sich strikt an den Vorgaben orientiert, der geeignetere Weg ist.</p> <p>Etablieren Sie für die Zukunft einen internen Prozess zur Überwachung der KBA-Mindestanforderungen, durch den Änderungen der Vorgaben erkannt und geeignet behandelt werden können.</p>
--	---

<h1 style="font-size: 48px; margin: 0;">H</h1> <p style="font-weight: bold; margin: 5px 0 0 0;">high</p>	3. H – Unvollständige interne Übersicht über i-Kfz Komponenten		Elaborate	Complex	Simple
	Fehlerklasse: <i>Mangelnde Systempflege</i>	Grave		X	
	Serious				
	Light				
Betroffene Systeme:	Übergreifender Befund (u.a. Dezentrales Portal, Systeme der Fachverfahren)				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Im Rahmen der Prüfung konnte keine vollständige Übersicht aller i-Kfz-relevanten Systeme ermittelt oder bereitgestellt werden. Eine vollumfängliche Sicherheitsprüfung der Komponenten konnte daher nicht verbindlich durchgeführt werden.</p> <p>Teilweise existierten Netzpläne zu Teilbereichen (z.B. OSI Plattform), die aber nicht vollständig waren. Im Rahmen des Projekts wurde versucht, eine Übersicht über alle beteiligten Systeme zu erstellen. Trotz mehrerer Abstimmungsrunden und E-Mails zu dem Thema gab es bis zum Schluss noch Anpassungen und Ergänzungen der Liste.</p> <p>Die bereitgestellten Informationen waren im Hinblick auf die folgenden Punkte problematisch:</p> <ul style="list-style-type: none"> - Vollständigkeit der Systeme und Verbindungen, z.B. im Hinblick auf <ul style="list-style-type: none"> o Interne Verbindungen o Verbindungen zum KBA o Beteiligte Netzwerkkoppelemente o Übergreifende Multiverfahrensdienste - Aktualität der Übersichten (z.B. wiederholte widersprüchliche Aussagen zur Existenz eines DOI Netscaler) - Unklarheiten über Zugehörigkeiten <ul style="list-style-type: none"> o Teilweise konnte nicht ermittelt werden, ob ein System tatsächlich vorhanden oder an einer Kommunikationsstrecke beteiligt war - Zuordnung der Systeme zu i-Kfz-Schnittstellen 				

	<p>Sofern eine Übersicht über die i-Kfz-Komponenten intern existiert, so konnte Sie im Rahmen der Prüfung nicht geeignet bereitgestellt werden und waren mindestens den befragten Ansprechpartnern nicht bekannt.</p> <p>Kurz nach dem eigentlichen Ende der Prüfung wurde noch ein Schnittstellenkonzept bereitgestellt (laut Dokument „Version 1.2. vom 13.08.2021). Dieses enthält einen Teil der Schnittstellen und verweist für andere auf ein Sicherheitskonzept der Fachverfahren (vgl. „Sie ist im Sicherheitskonzept der Fachverfahrens beschrieben und von daher nicht Bestandteil dieses Konzeptes.“). Es enthält keine Übersicht der tatsächlich beteiligten Systeme (z.B. Hostnamen und Kommunikationsverbindungen). Im Rahmen der Prüfung konnte nicht mehr geklärt werden, warum dieses Dokument erst nach Ende der aktiven Prüfungen bereitgestellt wurde.</p>
Auswirkung:	<p>Eine fehlende Übersicht über relevante Komponenten erschwert die Verwaltung, Prüfung und Absicherung der Systeme enorm. Sofern intern nicht bekannt ist, welche Systeme Teil der i-Kfz-Architektur sind und welche Rolle sie darin einnehmen, können auch die KBA-Mindestanforderungen nicht gezielt umgesetzt werden. Das Sicherheitsniveau der Komponenten bleibt dadurch hinter den geforderten Mindestanforderungen zurück und ist als nicht ausreichend zu betrachten.</p>
Empfehlung:	<p>Prüfen Sie, ob eine interne Stelle existiert, welche die übergreifende Verantwortung über die i-Kfz-Systeme und –Prozesse hält oder schaffen Sie diese andernfalls. Diese Stelle sollte Zugriff auf alle notwendigen Dokumentationen erhalten oder wissen, an welcher Stelle diese vorgehalten wird. Auch sollte diese darüber auskunftsfähig sein, welche Entscheidungen mit i-Kfz-relevanten Inhalten in der Vergangenheit beschlossen wurden, welche Maßnahmen durchgeführt wurden (z.B. vergangene Penetrationstests), welche Ergebnisse diese hatten und wie der aktuelle Status ggf. offener Punkte ist.</p> <p>Die zentrale Stelle sollte dafür sorgen, dass eine geeignete Übersicht über alle i-Kfz-Komponenten existiert und sichergestellt bzw. nachverfolgt wird, dass alle internen und externen Anforderungen eingehalten werden. Beachten Sie in diesem Rahmen auch die Empfehlungen der anderen Befunde, wie beispielsweise Befund 4.</p>
Referenzen:	

<h1 style="font-size: 2em; margin: 0;">H</h1> <p style="font-weight: bold; margin: 0;">high</p>	4. H – Mangelhafte zentrale Übersicht über notwendige oder erlaubte i-Kfz-Kommunikationsverbindungen		Elaborate	Complex	Simple
		Grave		X	
	Fehlerklasse: <i>Mangelnde Systempflege</i>	Serious			
		Light			
Betroffene Systeme:	Übergreifender Befund (u.a. Dezentrales Portal, Systeme der Fachverfahren)				

Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.
Sachverhalt:	<p>Im Rahmen der Prüfung konnte keine vollständige Übersicht aller i-Kfz-relevanten Kommunikationsverbindungen ermittelt oder bereitgestellt werden, was u.a. daran lag, dass Systemzugehörigkeiten nicht bekannt oder nicht dokumentiert waren. Eine vollumfängliche Sicherheitsprüfung der KBA-Anforderungen konnte daher nicht durchgeführt werden.</p> <p>Trotz mehrfacher Anforderung konnte den Prüfern keine Übersicht zur Verfügung gestellt werden, welche Systeme auf welche Art und Weise (z.B. Ports und Protokolle) mit welchen anderen Systemen oder Komponenten kommunizieren. Eine solche Übersicht sollte auf Basis der Anwendungs- und Sicherheitsanforderungen erstellt und dann entsprechend umgesetzt werden. Gleichzeitig gilt dieses als Grundlage für eventuell einzurichtende Firewall-Freischaltungen und ermöglicht, dass diese auf Anfrage auf Gültigkeit und Notwendigkeit überprüft werden können.</p>
Auswirkung:	Durch die fehlende Übersicht der notwendigen oder bestehenden Kommunikationsverbindungen konnten die übergreifenden Firewall-Regeln nicht gezielt geprüft werden. Zudem konnte dadurch nicht verifiziert werden, dass alle i-Kfz-relevanten IT-Komponenten identifiziert und im Audit betrachtet werden konnten (siehe Befund 3).
Empfehlung:	<p>Erstellen Sie eine zentral gepflegte Übersicht über alle notwendigen Kommunikationsverbindungen der i-Kfz-relevanten IT-Komponenten.</p> <p>Prüfen Sie anschließend, wie sich diese Verbindungen über die vom KBA geforderten Netzbereiche, Komponenten und Schnittstellen realisieren lassen und setzen Sie diese entsprechend um. Beachten Sie dazu die Hinweise auf Befund 5.</p> <p>Setzen Sie anschließend die KBA-Mindestsicherheitsanforderungen für die System- und Netzwerktechnische Trennung der Komponenten um und prüfen Sie, dass die bisherigen Firewall-Freischaltungen keine zusätzlichen Kommunikationsmöglichkeiten eröffnen.</p>

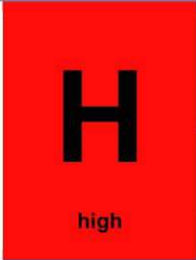
<div style="background-color: red; color: black; text-align: center; padding: 10px;"> <h1 style="margin: 0;">H</h1> <p style="margin: 0;">high</p> </div>	5. H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche		Elaborate	Complex	Simple
		Grave		X	
	Fehlerklasse: Anwendung: Design-Fehler	Serious			
		Light			
Betroffene Systeme:	Übergreifender Befund (u.a. Dezentrales Portal, Systeme der Fachverfahren)				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				

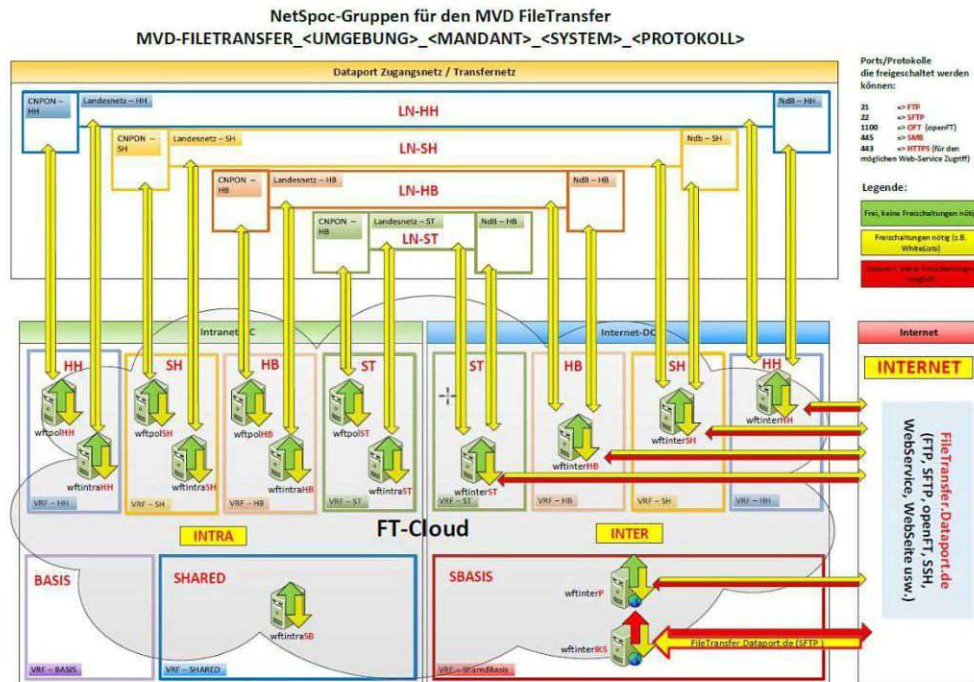
<p>Sachverhalt:</p>	<p>Der Betrieb der i-Kfz-Komponenten erfolgt nicht in den vom KBA geforderten separaten Netzbereichen. Damit einhergehend sind auch Zugriffsbeschränkungen nicht entsprechend der Vorgaben umgesetzt.</p> <p>Konkret sind die folgenden Netzbereiche nicht vorhanden oder problematisch:</p> <ul style="list-style-type: none">- „Dezentrales-Portal-DMZ“: Der Netzbereich setzt sich aus den beiden Bereichen „RZ² - Internet-DC“ und „RZ² - Intranet-DC“ zusammen“, welche beide übergreifend von der OSI-Plattform genutzt werden. Alle darin identifizierten i-Kfz-relevanten Systeme gehören zu Sub-Zonen der sogenannten „Standardsicherheit“. In Zonen der „Standardsicherheit“ gibt es zwischen den einzelnen Systemen der Sub-Zonen keine Zugriffsbeschränkungen für Verbindungen zwischen einander.- „Zulassungsbehörde-Kern-Netz“: Die Systeme der Fachverfahren sind ähnlich zu der „Dezentrales-Portal-DMZ“ innerhalb von Sub-Zonen der „Standardsicherheit“ innerhalb des Netzbereiches „RZ² - Intranet-DC“ angesiedelt. Zwar existieren darin verschiedene Sub-Zonen wie beispielsweise „Mandantenzone HH“ oder „Zugangszone SH“, eine Trennung durch Firewallregeln war jedoch nicht erkennbar.- „Zulassungsbehörde Internet DMZ“: Diese Zone wird bewusst nicht genutzt.- „Zulassungsbehörde-NdB-DMZ“: Die Komponente „Portal-NdB-Cnn“ existiert nicht in der geforderten Form, weshalb auch die Schnittstellen Xn und Yn nicht wie gefordert vorliegen. Die Kommunikation erfolgt direkt zwischen dem dezentralen Portal und Systemen der Fachverfahren.
<p>Auswirkung:</p>	<p>Die System- und netztechnische Sicherheit kann nicht nach den Vorgaben des KBA sichergestellt werden, wenn die dort geforderten Netzbereiche nicht oder nur unzureichend getrennt und die Anforderungen nur unzureichend umgesetzt sind.</p> <p>Ohne explizite Genehmigung vom KBA ist damit eine Zulassung der aktuellen Architektur fraglich, was im Falle eines Entzugs oder der Suspendierung der Zulassung erhebliche Auswirkungen auf den Betrieb und deren verbundenen Stellen und Dienste hat.</p>
<p>Empfehlung:</p>	<p>Erstellen Sie die Netzbereiche nach dem KBA-Referenzmodell und betreiben Sie dann nur diejenigen Systeme in den jeweiligen Netzbereichen, die vom KBA dort vorgesehen sind und i-Kfz-relevant sind. Andere Systeme dürfen keine Verbindungen zu den Systemen besitzen, sofern diese nicht speziell abgesichert und im i-Kfz-Sicherheitskonzept betrachtet wurden.</p> <p>Stellen Sie sicher, dass zwischen den Systemen nur die vom KBA erlaubten Kommunikationsverbindungen möglich sind.</p>

<h1 style="font-size: 48px; margin: 0;">H</h1> <p style="font-weight: bold; margin: 5px 0 0 0;">high</p>	6. H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen		Elaborate	Complex	Simple	
	Grave		X			
	Fehlerklasse: <i>Anwendung: Design-Fehler</i>	Serious				
	Light					
Betroffene Systeme:	Übergreifender Befund (u.a. Dezentrales Portal, Systeme der Fachverfahren)					
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.					
Sachverhalt:	<p>Die aktuelle Umsetzung der i-Kfz-Architektur enthält mehrere der geforderten Schnittstellen nicht oder nur in abweichender Form, wodurch die vom KBA geforderten Mindestsicherheitsanforderungen nicht eingehalten werden können.</p> <p><u>Schnittstellen Xn und Yn:</u></p> <p>Der Auftraggeber verwendet beabsichtigt die Komponente „Internet-Cnn“ nicht. Die alternativ geforderte Komponente „Portal-NdB-Cnn“ liegt allerdings ebenfalls nicht in der geforderten Form vor. Stattdessen findet die Kommunikation zwischen dem dezentralen Portal und den Systemen der Fachverfahren direkt statt. Da die Komponente nicht verwendet wird, werden auch die Schnittstellen Xn und Yn nicht in der geforderten Form betrieben und abgesichert.</p> <p><u>Schnittstelle A:</u></p> <p>Für die Authentisierung der BackendWS Komponente gegenüber den KBA WS per HTTP Basic Authentication müssen die aktuellen Zugangsdaten (Benutzerkennung und Passwort) der anfragenden Zulassungsstelle verwendet werden. Das KBA sieht dabei die Verwendung des Passwort-Webservices (oder auch "Web-Service Pass" in manchen KBA Dokumenten genannte) vor, der automatisch für die notwendigen und regelmäßigen Passwortänderungen verwendet werden kann. Dies ist im i-KFZ Online-Dienst noch nicht umgesetzt.</p> <p><u>Schnittstelle C:</u></p> <p>Im Rahmen der Prüfung konnte nicht abschließend geklärt werden, ob die Komponente „KBA-NdB-Cnn“ existiert und der geforderten Form entspricht. Falls ein System existiert, welche die Funktion der Komponente übernimmt, so gehört diese vermutlich zum Multiverfahrensdienst (MVD) „Dateitransfer“. Die Schnittstelle C wird entgegen der Anforderungen nicht aus dem Bereich Zulassungsbehörde-NdB-DMZ angeboten, sondern läuft direkt auf einem System der Fachverfahren (Batch und Reporting Server).</p> <p>Zu Beginn lag beim Auftraggeber keine Dokumentation vor, wo genau sich die Schnittstelle C überhaupt befindet. Nach mehreren Gesprächen wurde ein Multiverfahrensdienst vorgestellt, welcher anwendungsübergreifend Dateitransfers über verschiedene Netzgrenzen hinweg realisiert. Dieser führte zu dem Zeitpunkt auch die Kopiervorgänge zwischen Schnittstelle C und D durch.</p> <p>Dem Ansprechpartner des Multiverfahrensdiensts waren die zusätzlichen KBA-Anforderungen nicht bekannt.</p>					

	<p>Im Gespräch wurde argumentiert, dass ein Teil der MVD als Teil der Systeme der Fachverfahren oder indirekt am Zulassungsprozess beteiligten Verfahren angesehen werden könnte und ein zweiter Teil als der KBA-Connector „KBA-NdB-Cnn“. Diese Definition würde die vom KBA geforderten Kommunikationsrichtungen theoretisch einhalten. Dann würde aber weiterhin ein drittes System (Control-M) existieren, welche beide Komponenten anspricht und die verschiedenen Jobs darauf auslöst. Auch wären im derzeitigen Zustand der MVD die Abgrenzungen zu den anderen Anwendungen des Auftraggebers nicht gegeben und die zusätzlichen Anforderungen des KBA höchstens zufällig erfüllt.</p> <p><u>Schnittstelle F:</u></p> <p>Im Schnittstellekonzept, welches nach Ende der aktiven Prüfungen noch zur Verfügung gestellt wurde, wird der VPN-Router an der Kopfstelle AHZ vom Auftraggeber als Schnittstelle F spezifiziert. Die gleiche Schnittstelle wird laut dem Dokument für verschiedene weitere Test-, Entwicklungs- und Produktivsysteme genutzt. Der VPN-Router baut zwar eine gesicherte VPN-Verbindung zu dem KBA auf, bietet aber technisch gesehen keine dedizierte Schnittstelle zur Annahme und Weiterleitung von Nachrichten im XML-Format an. Es ist daher fraglich, ob die aktuelle Architektur den Anforderungen des KBA in diesem Aspekt genügt.</p> <p>Die Protokolldaten der Schnittstelle werden an einen zentralen Syslog-Server weitergeleitet. Die Speicherzeit beträgt aktuell 31 Tage, wobei diese pro Mandant angepasst werden könnte. Laut KBA-Anforderung A-6.2.6-3 müssen die Protokolldaten 6 Monate aufbewahrt werden.</p> <p><u>Schnittstelle H:</u></p> <p>Im Rahmen des Projekts wurden die Fragen zu den Sicherheitsanforderungen der Schnittstelle H anfangs nur unzureichend beantwortet, weshalb mangels Nachweis davon ausgegangen werden musste, dass diese in folgenden Punkten nicht erfüllt werden:</p> <ul style="list-style-type: none">- Protokollierung von Zugriffen- Inhalte der Protokolle- Speicherzeit der Protokolldaten- Protokollierung der stattgefundenen elektronischen Identitätsnachweise <p>Im Rahmen der Nachlieferung nach dem Ende der aktiven Prüfungen konnten zumindest die Inhalte der Protokolle sowie die generelle Vorgehensweise betrachtet werden.</p> <p>Dabei wurde festgestellt, dass die Log-Dateien über die Anwendung nur für standardmäßig 31 Tage einsehbar sind. Diese Zeitspanne kann pro Mandant angepasst werden. Technische Logdateien werden so lange aufbewahrt, wie ausreichend Speicher verfügbar ist. Dies sind aktuell etwa drei Wochen. Sowohl die aktuelle Zeitdauer als auch der generelle Umgang hinsichtlich der Speicherdauer entsprechen nicht den KBA-Anforderungen A-6.2.7-4.</p>
Auswirkung:	Wenn intern die Speicherdauer von Logdaten nicht bekannt oder nicht fest definiert ist, können auch die Sicherheitsanforderungen nicht gezielt umgesetzt und überprüft werden. Dadurch entsteht ein unkalkulierbares Risiko für die Sicherheit der Verbindung zum KBA sowie die Vertraulichkeit und Integrität der übertragenen Daten.

	Durch die nicht-Beachtung der Anforderungen ergeben sich mehrere Abweichungen von den KBA-Anforderungen beispielsweise in Bezug auf die Kommunikationsrichtungen zu den Schnittstellen.
Empfehlung:	<p>Auftraggeberseitig sollte eine genaue Übersicht erstellt werden, welche Komponenten der IT-Infrastruktur welche Rollen der i-Kfz-Architektur übernehmen und welche weiteren Systeme zusätzlich beteiligt sind oder Sonderrollen übernehmen. Sämtliche Kommunikationswege sollten in einer zentralen Kommunikationsmatrix dokumentiert werden und technisch auf diese dokumentierten Wege beschränkt werden.</p> <p>Die Sicherheitskonzepte für die Systeme oder die i-Kfz-Architektur sollte detailliert beschreiben, wie die vom KBA geforderten Anforderungen umgesetzt werden und welche zusätzlichen Sicherheitsmaßnahmen getroffen wurden.</p>

	7. H – Schnittstelle C mit Fremd-Administratoreingriff		Elaborate	Complex	Simple
		Grave		X	
	Fehlerklasse: Anwendung: Design-Fehler	Serious			
		Light			
Betroffene Systeme:	Multiverfahrensdienst, wiatqw01 + wiatpw001				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	Entgegen der Vorgaben werden Daten nicht vom Fachverfahren von der Schnittstelle C (dem Datenaustauschdienst) abgeholt, sondern vom Multiverfahrensdienst (MVD) auf eine SMB-Freigabe des Fachverfahrens eingespielt.				



Die Steuerung der OpenFT-Server und auch des ViatoZ-Server erfolgt über einen zentralen Control-M Server und entsprechende Agents. Ein solcher läuft auch auf dem Batch&Reporting-Server.

Der Zugriff erfolgt mit dem Account `MGMT\D-CTM-SVC` der lokaler Administrator ist.

Auswirkung:	<p>Die Initiierung der Verbindung erfolgt entgegengesetzt zur Vorgabe des KBA.</p> <p>Da der genutzte Account ein lokaler Administrator ist und eingehende angemeldete Verbindungen eine RemoteShell aufrufen dürfen (siehe auch 211 – Härtingen ohne Herleitung) kann der Multiverfahrensdienst den Server und die darauf gespeicherten Daten beliebig ändern.</p>
Empfehlung:	<p>Die Zugriffsrichtung sollte umgedreht werden, so dass der MVD keinerlei Zugriff mehr auf das Fachverfahren hat, sondern dieses auf entsprechende Freigaben zugreift.</p> <p>Die dann nicht mehr notwendigen Freigabe und Administrator-Account sollte gelöscht werden.</p>

<h1 style="font-size: 48px; margin: 0;">M</h1> <p style="font-weight: bold; margin-top: 10px;">medium</p>	8. M – Zugriffsweg und Absicherung Schnittstelle D unbekannt		Elaborate	Complex	Simple
		Grave	X		
	Fehlerklasse: Anwendung: Design-Fehler	Serious			
		Light			
Betroffene Systeme:	Sicherheits-Proxy und NdB-Router				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Der Zugriffsweg auf Schnittstelle D ist nicht nachvollziehbar.</p> <p>Laut Dokumentation erfolge der Zugriff auf KBA-Systeme über einen Sicherheitsproxy (gelegentlich als „DOI-Netscaler“ benannt), der aber nicht verortet werden konnte. Dieser leitet eine intern genutzte URL weiter zum KBA - oder anderen Systemen (abhängig von der Aufruf-URL).</p> <p>Der Proxy unterscheidet dabei nicht, von welcher Quell-Adresse der Zugriff erfolgt.</p>				
Auswirkung:	Systeme die Firewall-seitig z.B. auf/über den Sicherheitsproxy auf andere Ziele (z.B. die PaymentAPI) zugreifen dürfen, können auch auf den KBA-Zugang (serviceconnector) zugreifen.				
Empfehlung:	Abhängig von den Möglichkeiten des Sicherheitsproxys sollten <ul style="list-style-type: none"> Sprungziele nur abhängig von der Quell-IP-Adresse weitergeleitet werden 				

- für den KBA-Zugang ein dedizierter Proxy mit eigener IP-Adresse eingerichtet werden.

Grundsätzlich sollten sämtliche sicherheits- und zulassungsrelevanten Konfigurationen und Verantwortlichkeiten des i-KFZ Verfahrens sowie die entsprechenden Ansprechpartner der Fachabteilung bekannt sein.

5 ERGEBNISSE DES EXTERNEN PENETRATIONSTESTS

Der externe Penetrationstest wurde am 02.08.2021 durchgeführt.

5.1 Getestete Systeme und Netzbereiche

- serviceportal-stage.hamburg.de (141.91.183.233)
- serviceportal-stage.schleswig-holstein.de (141.91.183.231)

5.2 Vorgehen

Tabelle 4: Durchführung des externen Penetrationstests

Testschritt	Beschreibung
Ermittlung von aktiven Systemen und Ports	Durch den Einsatz der Werkzeuge Hping und Nmap wurden die aktiven Systeme in dem Adressbereich ermittelt, deren offene Ports identifiziert und deren Dienste bestimmt.
Schwachstellenanalyse der aktiven Systeme	Die ermittelten Systeme wurden einer Schwachstellenanalyse mit dem Werkzeug Nessus unterzogen.
Manuelle Penetration	Alle Feststellungen aus der automatischen Überprüfung der Systeme wurden manuell verifiziert und soweit mit dem Kunden abgestimmt ausgenutzt, um auf die Systeme zuzugreifen. Es wurden nur frei verfügbare Exploits eingesetzt. Die Entwicklung von eigenen Exploits für die gefundenen Schwachstellen, für die es keine frei verfügbaren Exploits gibt, war nicht beauftragt.

5.3 Verwendete Werkzeuge

Tabelle 5: Eingesetzte Software im Penetrationstest

Name	URL
Nessus	https://www.tenable.com/products/nessus/nessus-professional
Nmap	https://nmap.org/

5.4 Ergebnisse

Die folgende Tabelle zeigt die im untersuchten Netzbereich gefundenen Systeme.

Tabelle 6: Aus dem Internet erreichbare Systeme und Dienste

IP	DNS	Port	Dienst	Bemerkungen
141.91.183.231	serviceportal-stage.schleswig-holstein.de	80/tcp	HTTP	
141.91.183.231		443/tcp	HTTPS	

141.91.183.233	serviceportal-stage.hamburg.de	80/tcp	HTTP
141.91.183.233		443/tcp	HTTPS

Aus dem Test ergaben sich folgende Befunde auf Infrastruktur-Ebene (die Web-Anwendungen wurden in Kapitel geprüft):

OK	9. OK – Keine unnötige Angriffsfläche		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse: <i>Info / Funktionalität</i>	Serious			
		Light			
Sachverhalt:	Für die geprüften Systeme waren nur die Ports über das Internet erreichbar, welche für die Funktion der Web-Portale sinnvoll waren. Bei der SSL-Konfiguration konnten ebenfalls keine Probleme festgestellt werden.				
Auswirkung:	Für die geprüften IP-Adressen besteht kein erhöhtes Angriffsrisiko durch zusätzlich exponierte oder unsicher konfigurierte Dienste.				
Empfehlung:	Prüfen Sie, ob die Staging-Umgebungen generell überhaupt aus dem Internet erreichbar sein müssen und sperren Sie den Zugriff gegebenenfalls.				

6 PRÜFUNG DER WEBANWENDUNGEN – IS-WEBCHECK

Der Prüfung wurde im Zeitraum vom 02.08.2021 bis zum 03.08.2021 **über das Internet** durchgeführt. Die Prüfung wurde **ohne ein vorgeschaltetes Sicherheitsgateway** durchgeführt. Die Basis der Prüfung bildete ein **nicht invasiver Schwachstellenscan** der Web-Anwendungen. Für Formularfelder und Eingabemöglichkeiten erfolgten Angriff mit dem **Ziel einer Ausnutzung**, allerdings auf nicht invasive und nicht destruktive Weise.

6.1 Getestete Seiten

Der IS-Webcheck wurden mit einem Fokus auf die i-Kfz-relevanten Bestandteile der Serviceportale der Mandaten Hamburg und Schleswig-Holstein durchgeführt. Es wurde nicht die gesamte Funktionalität der Serviceportale untersucht oder geprüft. Die folgenden Serviceportale wurden betrachtet:

- <https://serviceportal-stage.hamburg.de/> (141.91.183.233)
- <https://serviceportal-stage.schleswig-holstein.de/> (141.91.183.231)

Verlinkte Seiten mit Inhalten anderer URLs wurden vom Test ausgeschlossen.

6.2 Einschränkungen

Während des Tests wurden nur die i-Kfz-relevanten Bestandteile der Serviceportale geprüft. Dies beinhaltet u.a. die URLs unterhalb von:

- <https://serviceportal-stage.schleswig-holstein.de/Verwaltungsportal/FVP/FV/ITVSH/IKFZSH/>
- <https://serviceportal-stage.schleswig-holstein.de/Verwaltungsportal/FVS/FV/ITVSH/WUKENNZSH>
- <https://serviceportal-stage.hamburg.de/HamburgGateway/FVP/FV/LBV/IKFZ/>

Im zur Verfügung stehenden Zeitrahmen war es nicht möglich, die kompletten Web-Anwendungen zu prüfen, da dort nach Aussagen des Auftraggebers bis zu 500 weitere Dienste auf der gleichen Plattform (OSI) betrieben werden. Im Vorfeld des Tests wurde vereinbart, dass der Auftraggeber mit dem KBA die weitere Vorgehensweise abstimmt und danach gegebenenfalls weitere Tests durchgeführt werden.

6.3 Vorgehen

Die durchgeführten Tests decken auch die vom OWASP-Projekt 2017 veröffentlichten „OWASP Top Ten“ ab. Die Befunde werden in davon abgeleitete Fehlerklassen eingeteilt. Siehe hierzu die entsprechende Darstellung im Anhang A.

Tabelle 7: Durchführung des Web-Sicherheitstests

Testschritt	Beschreibung
Schwachstellenanalyse	<p>Mit verschiedenen Tools wurden die Webseiten abgerufen und die Antworten und der gelieferte HTTP-Header untersucht. Gesucht wurde u.a. nach Hinweisen auf interne Systeme, Versionsnummer, Parameter in den Headern und mögliche Request-Typen.</p> <p>Ebenso wurden nach Schwachstellen in den folgenden Aspekten gesucht:</p> <ul style="list-style-type: none">- Korrektes Verhalten der Webanwendung

- Aktualität der Patchstände und der eingesetzten Softwareversionen
- Verschlüsselung entsprechend der aktuellen Sicherheitsanforderungen
- Unerwünschte Informationspreisgabe
- Eingabe und Interaktionsmöglichkeiten

Schwachstellentest

Die Web-Anwendungen und Eingabemöglichkeiten wurden auf klassische Schwachstellen u.a. der OWASP-Top 10 untersucht. Dabei wurde betrachtet:

- Eingabevalidierung
- Session Handling
- Zugriffskontrolle
- Verschlüsselung
- Fehlerhandling
- Absicherung der beteiligten Datenbanken und Anwendungen
- Absicherung von Dateiuploadmöglichkeiten und weiteren Interaktionsmöglichkeiten
- versteckte Parameter/Verzeichnisse

Logische Fehler/Konfigurationsfehler

In der Anwendung wurden gezielt Fehlerzustände herbeigeführt, um technische Informationen über den Untersuchungsgegenstand zu gewinnen, die für weitere Tests hilfreich sein können. Die Anwendungslogik wurde auf Fehler untersucht, welche zum Umgehen von Sicherheitsmaßnahmen oder beispielsweise dem Überspringen von Schritten genutzt werden können. Zusätzlich wurden die Web-Anwendungen untersucht auf:

- Fehler beim Aufbau oder Konfiguration z. B. des HTTP-Protokoll
- Mögliche Seiteneffekte

Exploits

Alle Feststellungen aus der automatischen Überprüfung der Systeme wurden manuell verifiziert. Wo sinnvoll wurden Exploits beispielsweise zum Nachweis von XSS-Schwachstellen erstellt und für den Bericht dokumentiert.

Die Entwicklung von eigenen Exploits für die gefundenen Schwachstellen, für die es keine frei verfügbaren Exploits gibt, war nicht beauftragt.

6.4 Verwendete Werkzeuge

Tabelle 8: Eingesetzte Software im Web-Sicherheitstest

Name	URL	Version
Burp Suite	https://portswigger.net/burp	2021.6.2
IIS Short Name Scanner	https://github.com/irsdl/IIS-ShortName-Scanner	2.3.9
Kali Linux	https://www.kali.org/	2021.3
Nessus	https://www.tenable.com/products/nessus/nessus-professional	8.13.0
Nikto	https://cirt.net/Nikto2	2.1.5
Nmap	https://nmap.org/	7.91

6.5 Ergebnisse

Aus dem Test ergaben sich folgende Befunde:

<div style="font-size: 48px; font-weight: bold; margin: 0;">M</div> <div style="font-size: 12px; font-weight: normal; margin-top: 5px;">medium</div>	10. M – Ungenügender Schutz vor Cross-Site-Scripting (XSS) Angriffen		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse: <i>Client-side Injection (OWASP A7)</i>	Serious		X	
		Light			
Betroffene Systeme:	serviceportal-stage.hamburg.de, serviceportal-stage.schleswig-holstein.de				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Der Schutz der Portale vor Cross-Site-Scripting-Angriffen (XSS) ist ungenügend was in mindestens einem Fall für eine XSS-Schwachstelle sorgt. Durch einen XSS-Angriff kann der Angreifer JavaScript im Kontext des Benutzers ausführen. Damit kann er versuchen, Daten zu entwenden oder Session-Tokens zu stehlen, um sich als ein spezifischer Benutzer ausgeben zu können.</p> <p>Die Anwendung scheint sich größtenteils auf eine eingebaute .NET-Schutzfunktion, die sogenannte .NET Request Validation, zu verlassen um XSS-Schwachstellen zu verhindern. Diese Funktion erkennt, wenn gültige HTML-Tags in einer HTTP-Anfrage gesendet werden und leitet die Anfrage dann auf eine Fehlerseite um. Das Einfügen von ungültigen HTML-Tags wie „<script>“, welche aber in alten Browsern als Angriffsvektor genutzt werden können, ist an diversen Stellen der Anwendung möglich. Dies betrifft beispielsweise Fehlermeldungen, die innerhalb der Anwendung ausgegeben werden, wenn ein Eingabeparameter nicht dem erwarteten Wert entspricht.</p>				

Ein Beispiel dafür wäre die HTTP-Anfrage:

```
POST /HamburgGateway/FVP/FV/LBV/IKFZ/Dsgvo/Post HTTP/1.1
Host: serviceportal-stage.hamburg.de
...
Connection: close

__RequestVerificationToken=L5u-
BXUkBIJThsz8rSNKM3cwWzNhiKDPpbjwsRSxa6JKerW40mEAPKGoZi7ZC4nHIWljf1NEa
1lml4KWcHB-
480ZnXA1&Completed=true%3c%25GiBQQ%3e&Modified=false&DsgvoAcceptance=
true&DsgvoAcceptance=false
```

Die Antwort enthält dann die Fehlermeldung:

```
...
The value 'true<%GiBQQ>' is not valid for Completed.
...
```

Einer der Nachteile der reinen Verwendung dieser Schutzfunktion ohne weitere Maßnahmen zur Verhinderung von Cross-Site-Scripting-Angriffen ist, dass diese nicht greifen, wenn kein vollständiges HTML-Tag für einen Angriff eingefügt werden muss. Im Test wurde eine Funktion identifiziert, bei der die übergebenen Werte direkt in das href-Attribut eines Link-HTML-Tags eingefügt werden. Durch das Einfügen einer Zeichenkette, die mit dem Wert „javascript:“ beginnt, kann darüber beliebiger JavaScript-Code eingebettet werden. Der Code wird beispielsweise ausgeführt, wenn ein Nutzer eine manipulierte URL aufruft und dann den auf der Seite angezeigten Link anklickt.

Das Verhalten kann durch den Aufruf des folgenden Links reproduziert werden:

```
https://serviceportal-stage.schleswig-holstein.de/Verwaltungsportal/Render/SideBar?selectedMenuId=Entry&customMenu=%7B%22itemName%22%3A%22Weiter%20zum%20Login-Portal%22%2C%22itemLink%22%3A%22javascript%3Aalert%28document.cookie%29%2F%2Fzvga6w7v%22%7D&\_1627983242560
```

Nach dem Klicken auf den angezeigten Link, dessen Textbeschreibung beliebig vom Angreifer gewählt werden kann (hier „Weiter zum Login-Portal“), wird eine harmlose Dialogbox beim Benutzer angezeigt, welche als Beispiel für die Ausführung von beliebigen JavaScripts dient:

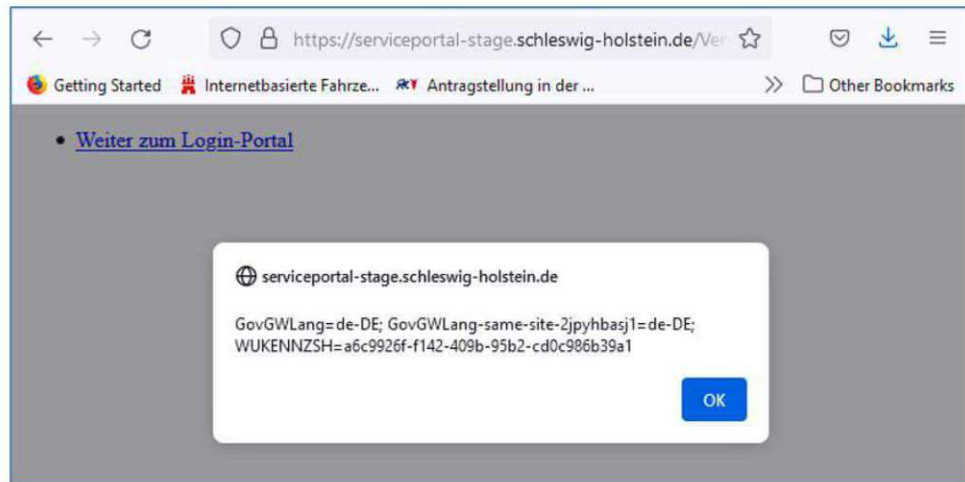



Abbildung 5: Screenshot des beispielhaften JavaScript Pop-Ups.

Der zweite Mandant ist durch die gleiche Plattform auf dieselbe Art und Weise anfällig:

https://serviceportal-stage.hamburg.de/HamburgGateway/Render/SideBar?selectedMenuId=Entry&customMenu=%7B%22itemName%22%3A%22Weiter%20zum%20Login-Portal%22%2C%22itemLink%22%3A%22javascript%3Aalert%28document.cookie%29%2F%2Fzvgaw7v%22%7D&_ =1627983242560

<p>Auswirkung:</p>	<p>Angreifer können JavaScript im Kontext des Benutzers ausführen, wenn der Benutzer auf einem manipulierten Link klickt oder eine vom Angreifer kontrollierte Seite besucht. Sie können dadurch Seiteninhalte ändern oder versuchen, persönliche Details und Zugangsdaten zu entwenden, die vom Benutzer eingegeben oder abgerufen werden.</p> <p>Reflektiertes Cross-Site-Scripting kann es Angreifern zudem erlauben, potenziell bösartige URLs zu generieren und diese beispielsweise als Link an Mitarbeiter zu versenden. Über solche Links können dann gezielte Phishing-Angriffe gestartet, oder über den Browser Schadcode ausgeführt werden.</p>
<p>Empfehlung:</p>	<p>Grundsätzlich sollten alle vom Nutzer beeinflussbaren Werte vor dem Einbinden in die Web-Anwendung geeignet gefiltert oder so codiert werden, dass kein Einfügen von HTML-Elementen oder Code-Fragmenten möglich ist. Welche Sonderzeichen dabei codiert oder gefiltert werden müssen, hängt stark von dem jeweiligen Ort ab, an welchen die Werte eingefügt werden. Bei Werten, die innerhalb von anderen HTML-Elementen wie <p>, <div> oder <td> eingefügt werden, sollten beispielsweise die Zeichen &, ", ', < und > codiert werden.</p> <p>Werden Funktionen der Web-Anwendungen zur dynamischen Generierung von HTML-Elementen (wie hier Header, Footer und Sidebar) genutzt, so muss ebenfalls sichergestellt werden, dass je nach Kontext kein Einfügen von schadhafte Inhalten möglich ist. Im Falle von dynamischen Links muss beispielsweise sichergestellt werden, dass der Inhalt nicht mit der Zeichenkette „javascript:“ oder einem Link zu einer externen Seite beginnt. Dies könnte beispielsweise darüber sichergestellt werden, dass in dem href-Attribut standardmäßig die URL des Portals, also z.B. „https://serviceportal-stage.hamburg.de/“ vorangestellt wird.</p>

	<p>Die Referenzen und Anhang B.1 Cross-Site-Scripting (XSS) geben weitere wichtige Hinweise zur generellen Beseitigung von Cross-Site-Scripting-Schwachstellen.</p> <p>Der Einsatz von ausreichend restriktiv definierten Content-Security-Policy HTTP-Headern bietet zusätzlichen Schutz gegen XSS-Angriffe.</p>
Referenzen:	<p>http://de.wikipedia.org/wiki/Cross-Site-Scripting</p> <p>https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASP-DV-002)</p> <p>https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet</p> <p>https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP</p> <p>Sicherheit von Webanwendungen BSI</p> <p>Anhang B.1 Cross-Site-Scripting (XSS)</p>

	<p>11.L – Detaillierte Fehlermeldungen geben interne Details preis</p>		Elaborate	Complex	Simple
		Grave			
	<p>Fehlerklasse: <i>Anwendung: Implementierungs-Fehler</i></p>	Serious	X		
		Light			
Betroffene Systeme:	serviceportal-stage.hamburg.de, serviceportal-stage.schleswig-holstein.de				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt				
Sachverhalt:	<p>Die Anwendungen geben an verschiedenen Stellen technische Details preis, welche Angreifer zur Vorbereitung oder Verfeinerung weitere Angriffe nutzen können.</p> <p>.NET-Fehlermeldungen (Stack-Traces):</p> <p>Durch gezielt manipulierte HTTP-Anfragen lassen sich Fehlermeldungen in der Anwendung provozieren, welche unverändert angezeigt werden. Diese enthalten teilweise schützenswerte Informationen, wie technische Details zur Anwendung sowie der Versionsnummern der eingesetzten Software.</p>				

Server Error in '/Verwaltungsportal/FVS/FV/ITVSH/WUKENNZSH' Application.

A potentially dangerous Request.Form value was detected from the client (AuswahllisteZulassungsstelle="...(xmlype('<?xml ve

Description: ASP.NET has detected data in the request that is potentially dangerous because it might include HTML markup or script. The data might represent an attempt to compromise the security of your application, such as a cross-site scripting see <http://go.microsoft.com/fwlink/?LinkId=212874>.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.Form value was detected from the client (AuswahllisteZulassungsstelle="...(xmlype('<?xml version="1.0" ...).

Source Error:

In unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (AuswahllisteZulassungsstelle="
System.Web.HttpRequest.ValidateString(String value, String collectionKey, RequestValidationSource requestCollection) +11778768
System.Web.HttpValueCollection.EnsureKeyValidated(String key) +11775741
System.Web.HttpValueCollection.GetValues(String name) +24
System.Web.Mvc.ValueProviderResultPlaceholder.GetResultFromCollection(String key, NameValueCollection collection, CultureInfo culture) +32
System.Web.Mvc.NameValueCollectionValueProvider.GetValue(String key, Boolean skipValidation) +129
System.Web.Mvc.ValueProviderCollection.GetValue(String key, Boolean skipValidation) +157
System.Web.Mvc.DefaultModelBinder.BindModel(ControllerContext controllerContext, ModelBindingContext bindingContext) +372
System.Web.Mvc.DefaultModelBinder.GetPropertyValues(ControllerContext controllerContext, ModelBindingContext bindingContext, PropertyDescriptor prop
System.Web.Mvc.DefaultModelBinder.BindProperty(ControllerContext controllerContext, ModelBindingContext bindingContext, PropertyDescriptor property
System.Web.Mvc.DefaultModelBinder.BindProperties(ControllerContext controllerContext, ModelBindingContext bindingContext) +164
System.Web.Mvc.DefaultModelBinder.BindComplexElementalModel(ControllerContext controllerContext, ModelBindingContext bindingContext, Object model)
System.Web.Mvc.DefaultModelBinder.BindComplexModel(ControllerContext controllerContext, ModelBindingContext bindingContext) +1942
System.Web.Mvc.ControllerActionInvoker.GetParameterValue(ControllerContext controllerContext, ParameterDescriptor parameterDescriptor) +446
System.Web.Mvc.ControllerActionInvoker.GetParameterValues(ControllerContext controllerContext, ActionDescriptor actionDescriptor) +137
System.Web.Mvc.Async.<.>c__DisplayClass31.1.<BeginInvokeAction>b__0(AsyncCallback asyncCallback, Object asyncState) +1882
System.Web.Mvc.Async.WrappedAsyncResultBase`1.Begin(AsyncCallback callback, Object state, Int32 timeout) +163
System.Web.Mvc.Async.AsyncControllerActionInvoker.BeginInvokeAction(ControllerContext controllerContext, String actionName, AsyncCallback callback
System.Web.Mvc.<.>c__BeginExecuteCore>b__152_0(AsyncCallback asyncCallback, Object asyncState, ExecuteCoreState innerState) +48
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallBeginDelegate(AsyncCallback callback, Object callbackState) +73
System.Web.Mvc.Async.WrappedAsyncResultBase`1.Begin(AsyncCallback callback, Object state, Int32 timeout) +163
System.Web.Mvc.Controller.BeginExecuteCore(AsyncCallback callback, Object state) +787
System.Web.Mvc.Async.WrappedAsyncResultBase`1.Begin(AsyncCallback callback, Object state, Int32 timeout) +163
System.Web.Mvc.Controller.BeginExecute(RequestContext requestContext, AsyncCallback callback, Object state) +638
System.Web.Mvc.<.>c__BeginProcessRequest>b__20_0(AsyncCallback asyncCallback, Object asyncState, ProcessRequestState innerState) +99
```

Abbildung 6: Screenshot eines beispielhaften Stack-Traces.

Ähnliche Fehler, welche von der Anwendung anscheinend nicht korrekt abgefangen werden, lassen sich an diversen weiteren Endpunkten und Parametern provozieren.

HTTP-Header und Standard-Fehlerseiten:


An mehreren Stellen geben HTTP-Header Hinweise auf die Versionsnummern der verwendeten Software. Dies zeigt die folgende beispielhafte Antwort, welche beim Aufruf der URL <https://serviceportal-stage.schleswig-holstein.de/Verwaltungsportal/FVS/FV/ITVSH/WUKENNZSH/%3f/> auf der Standard-Fehlerseite zurückgegeben wird:

```
HTTP/1.1 400 Bad Request
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
...
...
<b>Version Information:</b>&nbsp;&nbsp;&nbsp;Microsoft .NET Framework
Version:4.0.30319; ASP.NET Version:4.8.4330.0
```

Ähnliches Verhalten ist für 404- und 403-Seiten (z.B. <https://serviceportal-stage.schleswig-holstein.de/a%5c.aspx>) zu beobachten:











```
HTTP/1.1 404 Not Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
Date: Tue, 03 Aug 2021 06:09:27 GMT
ntCoent-Length: 1918
Strict-Transport-Security: max-age=157680000
Content-Length: 1918
...
...
```

Auswirkung:	<p>Angreifer erhalten Informationen zu den eingesetzten Software-Paketen und – Bibliotheken auf dem System. Detaillierte Fehlerinformationen können erforderliche Details zum Ausnutzen einer Schwachstelle preisgeben bzw. deren Ausnutzung erheblich vereinfachen. Beim Bestehen einer Schwachstelle erlaubt dies einen zielgerichteten Angriff und erhöht die Erfolgschancen eines Angreifers.</p> <p>Obwohl dieser Befund für sich selbst genommen keine ausnutzbare Schwachstelle darstellt, bieten die preisgegebenen Daten Anhaltspunkte für weiterführende Angriffe, weshalb HiSolutions den Befund als Schwachstelle mit zumindest geringer Sicherheitsauswirkung einstuft.</p>
Empfehlung:	<p>Prüfen Sie, ob die Stack-Traces lediglich in der Staging-Umgebung der Anwendungen angezeigt werden und deaktivieren Sie die Ausgabe von Fehlermeldungen im Produktivbetrieb. In der bereitgestellten Liste an Unterschieden zwischen Produktiv- und Staging-Umgebungen ist dieser Sachverhalt nicht aufgeführt. Ersetzen Sie internen Fehlermeldungen durch generische Texte, die nur notwendige und beschränkte Information an den Benutzer weitergeben. Bedenken Sie, dass ein Angreifer auch aus Stack-Traces in Test- und Entwicklungs-Umgebungen Hinweise über die Funktionsweise der Anwendungen sammeln und diese dann für Angriffe gegen die Produktivumgebung verwenden kann.</p> <p>Ersetzen Sie die Versionsnummern auf Fehlerseiten und in HTTP-Headern durch generische Werte oder deaktivieren Sie die HTTP-Header vollständig. Für IIS kann die Konfiguration der Fehlerseiten beispielsweise über die grafische Oberfläche (siehe Referenzen) oder direkt in der <code>web.config</code> Datei erfolgen.</p>
Referenzen:	<p>https://www.owasp.org/index.php/Improper_Error_Handling</p> <p>https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-3.0/h0hfz6fc(v=vs.85)?redirectedfrom=MSDN</p> <p>https://docs.microsoft.com/en-us/iis/configuration/system.webserver/httperrors/</p>

	<p>L – Unsichere Content-Security-Policy</p>		Elaborate	Complex	Simple
	<p>Grave</p>				
	<p>Serious</p>	<p>X</p>			
	<p>Light</p>				
Betroffene Systeme:	<p>serviceportal-stage.hamburg.de, serviceportal-stage.schleswig-holstein.de</p>				
Nachtest:	<p>Ein Nachtest wurde noch nicht durchgeführt.</p>				

<p>Sachverhalt:</p>	<p>Die durch die Anwendung gesetzte Content-Security-Policy erlaubt den Einsatz unsicherer JavaScript-Funktionen, was im Test zur einfachen Ausnutzung einer XSS-Lücke genutzt wurde.</p> <p>Die Anwendung für den Mandanten SH wird mit dem folgenden Content-Security-Policy-Header ausgeliefert:</p> <pre>Content-Security-Policy: default-src 'self';font-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de data;;connect-src 'self' 'unsafe-inline' 'unsafe-eval' *.dataport.de https://geoportal-hamburg.de *.bremen.de *.hamburg.de;style-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de 'unsafe-inline';media-src https://captcha.osi.dataport.de https://captcha.osi-stage.dataport.de https://captcha.osi.dsecure-bdc.dataport.de;img-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de geoportal-hamburg.de *.geodatenzentrum.de *.bremen.de *.hamburg.de http://geodienste.bremen.de data;;script-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de https://captcha.osi.dataport.de https://captcha.osi-stage.dataport.de https://captcha.osi.dsecure-bdc.dataport.de 'unsafe-inline' 'unsafe- eval';frame-src https://serviceportal-stage.schleswig-holstein.de/;</pre> <p>Der Header für den Mandanten HH ist analog definiert:</p> <pre>Content-Security-Policy: default-src 'self';font-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de data;;connect-src 'self' 'unsafe-inline' 'unsafe-eval' *.dataport.de https://geoportal-hamburg.de *.bremen.de *.hamburg.de;style-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de 'unsafe-inline';media-src https://captcha.osi.dataport.de https://captcha.osi-stage.dataport.de https://captcha.osi.dsecure-bdc.dataport.de;img-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de geoportal-hamburg.de *.geodatenzentrum.de *.bremen.de *.hamburg.de http://geodienste.bremen.de data;;script-src 'self' https://uicdn.osi-stage.dataport.de https://uicdn.osi.dataport.de https://captcha.osi.dataport.de https://captcha.osi-stage.dataport.de https://captcha.osi.dsecure-bdc.dataport.de 'unsafe-inline' 'unsafe- eval';frame-src https://serviceportal-stage.hamburg.de/;</pre> <p>Über Content-Security-Policy können Sicherheitsvorgaben für JavaScript realisiert werden. Die Technologie zielt auf einen besseren Schutz vor Cross-Site-Scripting Angriffen ab.</p>
<p>Auswirkung:</p>	<p>Der durch die Content-Security-Policy mögliche Schutz vor Cross-Site-Scripting-Angriffen wird in der vorliegenden Konfiguration nicht in vollem Ausmaß realisiert.</p> <p>Zwar wird das Nachladen und Einbinden von JavaScript-Dateien durch die Angabe <code>script-src 'self'</code> nur vom eigenen Server gestattet und durch zusätzliche Angaben auf einige weitere Server erweitert, allerdings erlaubt <code>unsafe-inline</code> die Verwendung von <code><script></code>-Elementen im HTML-Code, <code>javascript:-</code>URLs sowie inline Event-Handlemern und <code><style></code>-Elementen. Die erfolgreiche Ausnutzung der Cross-Site-Scripting-Schwachstellen in der Anwendung (siehe Befund 10) basiert auf solchen inline <code>javascript:-</code>URLs.</p>

	<p><code>unsafe-eval</code> erlaubt darüber hinaus die Verwendung der JavaScript-Funktion <code>eval()</code> und ähnlicher Funktionen, die den im übergebenen String enthaltenen Code ausführen und grundsätzlich als unsicher eingestuft werden (siehe Referenzen).</p> <p>Da es sich bei den abgeschalteten Mechanismen ausschließlich um zusätzliche Sicherheitsmechanismen (im Sinne einer „Defense-in-depth“ Strategie) handelt, und der primäre Fokus auf der Absicherung der Anwendung selbst liegen sollte, werten wir den Befund dennoch als „low“.</p>
Empfehlung:	<p>Prüfen Sie, wo in Ihrer Anwendung <code>eval()</code> oder Inline-Javascript verwendet wird und ersetzen Sie den Code durch sichere Varianten (siehe die letzten beiden Referenzen). Anschließend entfernen Sie <code>unsafe eval</code> und <code>unsafe inline</code> aus der <code>Content-Security-Policy</code>.</p>
Referenzen:	<p>Anhang B.1.4 Content Security Policy</p> <p>https://content-security-policy.com/</p> <p>https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src</p> <p>https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/eval#never_use_eval!</p> <p>https://content-security-policy.com/unsafe-inline/</p>

	<p>12. L – Verbesserungswürdiger Schutz von Cookies</p>		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse: <i>Sensitive Data Exposure (OWASP A3/A8)</i>	Serious			
		Light			
Betroffene Systeme:	serviceportal-stage.hamburg.de, serviceportal-stage.schleswig-holstein.de				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Die Anwendung auf dem Server setzt teilweise für Cookies die Flags <code>Secure</code> und <code>HttpOnly</code> nicht, wodurch diese einem unnötigen zusätzlichen Angriffsrisiko ausgesetzt werden.</p> <p>Ohne das Flags <code>Secure</code> werden die folgenden Cookies gesetzt:</p> <ul style="list-style-type: none"> - GovGWLang - IKFZ 				

	<ul style="list-style-type: none">- <code>__RequestVerificationToken_*</code> <p>Ohne das Flag <code>HttpOnly</code> werden die folgenden Cookies gesetzt:</p> <ul style="list-style-type: none">- <code>GovGWLlang</code>- <code>GovGWLlang-same-site-*</code>- <code>IKFZ</code> <p>Der Cookie „IKFZ“ wird beispielsweise beim Aufruf der URL https://serviceportal-stage.schleswig-holstein.de/Verwaltungsportal/FVP/FV/ITVSH/IKFZSH?sid=327 mit Hilfe des folgenden <code>Set-Cookie-Headers</code> gesetzt:</p> <pre>Set-Cookie: IKFZ=4599cba5-8d24-4c58-bfa8-e5f3910815ee; path=/ Set-Cookie: IKFZ=aa118d32-5fec-4cda-98b9-45cc08f995d9; path=/ Set-Cookie: __RequestVerificationToken_L1z1cndhbHR1bmdzcg9ydGFsL0ZWUC9Gvi9JVFZTSC 9JS0ZaU0g1=PpY6P80hujCU4IePAp8WYTUhtf8bJYOIyCbGeC8i4FmXCu3GAgnueSrKV OQqjZd946fHKEtD4DSBYDUecbBbcwM60A1; path=/; HttpOnly</pre> <p>Dieser enthält weder das <code>Secure</code>-Flag, das den Browser anweist, den Cookie nur über verschlüsselte HTTPS-Verbindungen zu versenden, noch das <code>HttpOnly</code>-Flag, das einen Zugriff per JavaScript auf das Cookie unterbindet.</p>
<p>Auswirkung:</p>	<p>Angreifer mit Zugriff auf die Netzwerkstrecke können die Cookie-Werte mitlesen und damit eventuell auf schützenswerte Daten zugreifen, wenn der Benutzer auf einen Link an die HTTP-Version der Webseite klickt oder diesen manuell eingibt, und die Cookie-Werte für die Durchführung schützenswerter Aktionen notwendig sind.</p> <p>Angreifer, denen es (z.B. durch eine Cross-Site-Scripting Schwachstelle, siehe Befund 10) gelingt, eigenen JavaScript-Code im Kontext eines anderen Nutzers auszuführen, kann dessen Cookie-Werte auslesen, wenn diese nicht als <code>HttpOnly</code> gesetzt wurden.</p> <p>Bei den betroffenen Cookies scheint es sich nicht direkt um Sitzungs-Cookies zu handeln, weshalb die Auswirkungen des Befundes niedriger einzuschätzen sind. Mindestens bei dem Cookie „<code>__RequestVerificationToken_*</code>“ scheint es sich aber um einen schützenswerten Cookie zu handeln, weshalb der Befund zumindest mit niedrigen Sicherheitsauswirkungen dokumentiert wird.</p>
<p>Empfehlung:</p>	<p>Setzen Sie die Cookies, wo möglich, mit den Flags <code>Secure</code> und <code>HttpOnly</code>. Die Verwendung des <code>Secure</code>-Flags impliziert allerdings auch, dass die Anwendung in Folge nicht mehr unverschlüsselt über HTTP verwendet werden kann.</p> <p>Beachten Sie, dass das Flag <code>HttpOnly</code> nur für Cookies gesetzt werden kann, auf welche nicht per JavaScript zugegriffen werden muss. Das Setzen des Flags würde dies ansonsten verhindern um die Cookie-Werte vor unberechtigtem Zugriff, beispielsweise bei XSS-Angriffen, zu schützen.</p>
<p>Referenzen:</p>	<p>https://en.wikipedia.org/wiki/Secure_cookies</p> <p>https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies#Secure_and_HttpOnly_cookies</p> <p>https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html</p>

<div style="font-size: 48px; font-weight: bold; margin: 0;">L</div> <div style="margin-top: 10px;">low</div>	13. L – Einsatz veralteter JavaScript Bibliotheken		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse: <i>Using Components with Known Vulnerabilities (OWASP A9)</i>	Serious	x		
		Light			
Betroffene Systeme:	serviceportal-stage.hamburg.de, serviceportal-stage.schleswig-holstein.de				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Die Anwendungen binden eine veralteten jQuery-JavaScript-Bibliothek ein, welche bei einer bestimmten Verwendung mehrere bekannte Schwachstellen aufweist.</p> <p>Beide Anwendungen setzen jQuery in Version 3.3.1 ein. Die JavaScript-Bibliothek ist unter der folgenden URL abrufbar:</p> <ul style="list-style-type: none"> - https://serviceportal-stage.schleswig-holstein.de/Verwaltungsportal/Content/OSI/Tenant/SH/Scripts/uissystem.min.js bzw. - https://serviceportal-stage.hamburg.de/HamburgGateway/Content/OSI/Tenant/HH/Scripts/uissystem.min.js <p>Diese Version weist drei bekannte Schwachstellen (CVE-2019-11358, CVE-2020-11022, CVE-2020-11023) auf, welche unter Umständen genutzt werden können um Cross-Site-Scripting-Angriffe gegen Nutzer der Anwendungen durchzuführen.</p>				
Auswirkung:	<p>Diese Bibliotheken haben bekannte Schwachstellen, die unter Umständen sogar Cross-Site-Scripting (XSS) Angriffe ermöglichen.</p> <p>Die Schwachstellen betreffen dabei die Funktionen <code>jQuery.htmlPrefilter</code> und <code>jQuery.extend</code>, welche aktuell nicht auf angreifbare Art und Weise eingesetzt werden. Der Befund wird daher mit niedrigen Sicherheitsauswirkungen aufgenommen, da nicht ausgeschlossen werden kann, dass in Zukunft eine anfällige Verwendung eingeführt wird und der Befund auf ein gegebenenfalls unzureichendes Patch-Management von Anwendungskomponenten deutet.</p>				
Empfehlung:	<p>Aktualisieren Sie die eingesetzten Software-Bibliotheken auf Versionen ohne bekannte Schwachstellen. Für jQuery wäre die aktuelle Version 3.6.0. Die Schwachstellen sind ab Version 3.5.0 behoben.</p> <p>Stellen Sie sicher, dass im Entwicklungsprozess eine regelmäßige und systematische Prüfung der verwendeten Bibliotheken auf bekanntgewordene Schwachstellen durchgeführt wird und verwundbare, fehlerhafte oder nicht mehr weiterentwickelte Bibliotheken durch neuere Komponenten ersetzt werden.</p>				

Referenzen:	CVE-2019-11358 , CVE-2020-11022 , CVE-2020-11023 https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities
-------------	---

7 INTERNER PENETRATIONSTEST

Der interne Penetrationstest wurde im Zeitraum vom 19.07.2021 bis 20.07.2021 aus den Büros von Dataport durchgeführt.

7.1 Getestete Systeme und Netzbereiche

Für den Test konnte durch Dataport teilweise keine Konnektivität zu den jeweiligen Systemen hergestellt werden. Für nicht erreichbare Systeme wurde anschließend eine vergleichbare Prüfung der Konfiguration vorgenommen.

Folgende Systeme wurden durch einen **nicht-invasiven Schwachstellenscan** untersucht:

- Host: 10.59.43.76 (wosixqw007.fhhnet.stadt.hamburg.de) Status: Up
- Host: 10.59.143.77 (backendws-hh.stage.osi.dataport.de) Status: Up
- Host: 10.61.143.135 (payment.osi-stage.dataport.de) Status: Up
- Host: 10.62.130.102 (WVIATQW001.fhhnet.stadt.hamburg.de) Status: Up
- Host: 10.62.130.103 (wviatqw002.fhhnet.stadt.hamburg.de) Status: Up
- Host: 10.62.130.108 (wviatqd001.fhhnet.stadt.hamburg.de) Status: Up
- Host: 10.62.43.78 (wbmsqtd010.fhhnet.stadt.hamburg.de) Status: Up

Die folgenden Systeme waren trotz Freischaltung nicht erreichbar:

- Host: 10.61.101.15
- Host: 10.61.101.48
- Host: 10.61.127.233
- Host: 10.62.25.30
- Host: 10.62.25.36
- Host: 10.62.25.37
- Host: 10.62.25.44
- Host: 10.62.25.50
- Host: 10.62.127.10
- Host: 10.62.127.15
- Host: 10.62.127.16

Als alternative Prüfmethode wurde durch HiSolutions ein Skript erstellt, welches durch die zuständigen Administratoren auf den Systemen ausgeführt werden sollte. Die Ergebnisse des Skripts wurden anschließend durch HiSolutions ausgewertet. Das Skript hatte den folgenden Inhalt:

```
REM ComputerName
set CN=server0815

REM geht nur als admin
gpresult.exe /SCOPE COMPUTER /H %CN%_gpo-sys.html
netstat -an -b > %CN%_netstatp.txt

REM besser als admin
tasklist /v > %CN%_proc.txt

REM ginge auch als normaler User
```

```
systeminfo > %CN%_sys.txt
gpresult.exe /SCOPE USER /H %CN%_gpo-usr.html
wmic /output:%CN%_softw.txt product get name,version,installdate
wmic qfe list > %CN%_patches.txt
netsh advfirewall export %CN%_fw.txt
netstat -an > %CN%_netstat.txt
net user > %CN%_usr.txt
net localgroup > %CN%_groups.txt
net localgroup Administratoren> %CN%_locadm1.txt
net localgroup Administrators> %CN%_locadm2.txt
```

Die folgenden Systeme wurden mit diesem Skript untersucht:

- OSI-Plattform:
WOSIXQA005, WOSIXQW007, WOSIXQW012, WOSIXQW013, WOSIXQW014,
WOSIXQW015, WOSIXQW018, WOSIXQW020, WOSIXQW021
- ViatoZ-Server:
wviatqd001, wviatqw001, wviatqw002, wviatqw003

7.2 Einschränkungen

Eine Reihe an Systemen war aufgrund fehlender Freischaltungen gar nicht erreichbar und damit nicht im Rahmen eines Schwachstellenscans prüfbar. Weitere Systeme waren trotz Freischaltung nicht erreichbar, da der Netzwerkverkehr vom Büro Hamburg aus nicht in die entsprechenden Netze geroutet werden konnte.

Bei anderen Systemen, insbesondere aus dem 10.62.130.* Bereich, sorgte die installierte AntiVirus-Lösung für hohe Systemlast auf den Systemen (siehe Befund 19) - sowie entsprechende Einschränkungen bei Erkennungsraten beim Pentest.

7.3 Vorgehen

Tabelle 9: Durchführung des internen Penetrationstests

Testschritt	Beschreibung
Ermittlung von aktiven Systemen und Ports	Durch den Einsatz der Werkzeuge Hping und Nmap wurden die aktiven Systeme in dem Adressbereich ermittelt, deren offene Ports identifiziert und deren Dienste bestimmt.
Schwachstellenanalyse der aktiven Systeme	Die ermittelten Systeme wurden einer Schwachstellenanalyse mit dem Werkzeug Nessus unterzogen. Wo sinnvoll, wurden weitere detailliertere Scans durchgeführt um zusätzliche Angriffsfläche aufzudecken oder das Vorhandensein von Schwachstellen zu überprüfen.
Manuelle Verifikation	Die Ergebnisse der Scans wurden von den Prüfern auf mögliche Schwachstellen überprüft. Auf Basis dieses Überblicks über im Netzwerk vorhandene Systeme und Dienste wurden die weiteren Prüfschritte geplant und mit dem Auftraggeber abgestimmt.

Manuelle Penetration	<p>Alle verifizierten Feststellungen aus der automatischen Überprüfung wurden, soweit mit dem Kunden abgestimmt, ausgenutzt, um auf die Systeme zuzugreifen. Es wurden nur frei verfügbare Exploits eingesetzt.</p> <p>Die Entwicklung von eigenen Exploits für die gefundenen Schwachstellen, für die es keine frei verfügbaren Exploits gibt, war nicht beauftragt.</p>
Bewertung	<p>Alle Schwachstellen, deren Relevanz in der Verifikation bestätigt wurde, wurden anhand ihrer Kritikalität, der Auswirkungen eines Angriffs und der betroffenen Systeme und Daten bewertet und im Ergebnisbericht erläutert. Zur fachlichen Bewertung der Befunde und deren Auswirkung in der Praxis wurden diese jeweils bereits während der Tests mit dem Auftraggeber besprochen.</p> <p>Geeignete Gegenmaßnahmen wurden vorgeschlagen und sind im Bericht dargestellt.</p>

7.4 Verwendete Werkzeuge

Tabelle 10: Eingesetzte Software im internen Penetrationstest

Name	URL	Version
Burp Suite	https://portswigger.net/burp	2021.6.2
dirb	https://tools.kali.org/web-applications/dirb	2.22
Kali Linux	https://www.kali.org/	2021.3
Metasploit	https://www.metasploit.com/	6.0.18
Nessus	https://www.tenable.com/products/nessus/nessus-professional	8.13.0
Netcat	http://netcat.sourceforge.net/	1.10-46
Nikto	https://cirt.net/Nikto2	2.1.6
Nmap	https://nmap.org/	7.91
Wireshark	https://www.wireshark.org/	3.2.6

7.5 Ergebnisse

Aus dem Test ergaben sich folgende Befunde:

<h1 style="font-size: 48px; margin: 0;">H</h1> <p style="font-weight: bold; margin: 5px 0 0 0;">high</p>	14. H – Kritisch veralteter McAfee-Agent		Elaborate	Complex	Simple
		Grave		X	
	Fehlerklasse: <i>Using Components with Known Vulnerabilities (OWASP A9)</i>	Serious			
		Light			
Betroffene Systeme:	OSI-Plattform: WOSIXQA005, WOSIXQW007, WOSIXQW012, WOSIXQW013, WOSIXQW014, WOSIXQW015, WOSIXQW018, WOSIXQW020, WOSIXQW021 ViatoZ-Server: wviatqd001, wviatqw001, wviatqw002, wviatqw003				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	Auf den Systemen ist der McAfee-Agent in Version 5.06.0202 installiert (Installationsdatum 12/2019 für OSI, 12/2020 für ViatoZ). Es fehlen seit 12/2018 mehrere von McAfee als „Obligatorisch“ markierte Updates seit der installierten und schon bei Installation veralteten Version 5.06.0202				
Auswirkung:	Laut McAfee: <ul style="list-style-type: none"> • Wenn obligatorische Aktualisierungen nicht angewendet werden, kann dies zu einer Sicherheitsverletzung führen. • Mit obligatorischen Aktualisierungen und HotFixes werden Schwachstellen behoben, die sich auf die Produktfunktionalität auswirken und die Sicherheit beeinträchtigen können. Zusätzlich deutet dies auf ein unvollständiges Patchmanagement hin. Für die veralteten Agents sind zahlreiche (Remote) Code-Execution und Privilege-Escalation-Schwachstellen bekannt.				
Empfehlung:	Die veraltete Agent-Software sollte dringend aktualisiert werden. Zusätzlich sollte das Patch-Management überprüft werden, ob sämtliche installierte Software enthalten ist. Der McAfee-Agent ist in ein reguläres Patchmanagement aufzunehmen.				
Referenzen:	https://kc.mcafee.com/corporate/index?page=content&id=KB51573 https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=McAfee%20Agent				

<div style="font-size: 48px; font-weight: bold; margin: 0;">M</div> <div style="font-size: 12px; margin-top: 5px;">medium</div>	15. M – Microsoft SQL-Server veraltet		Elaborate	Complex	Simple
	Grave				
	Serious		X		
	Light				
Betroffene Systeme:	wwiatqd001 wwiatqw001				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	Auf beiden Servern ist das Softwarepaket „Microsoft SQL Server 2008 Setup Support Files“ installiert. Der Support für SQL-Server 2008 endete vor 2 Jahren. Die Installation von SQL Server 2012 ist mit Version 11.2.5058.0 (07/2015) ebenfalls stark veraltet.				
Auswirkung:	Es konnte im Rahmen der Untersuchungen nicht festgestellt werden, ob SQL Server 2008 noch betrieben wird, oder nur Installationsreste gefunden wurden. Für SQL-Server 2008 sind Remote Code-Execution Schwachstellen bekannt. Für den SQL-Server 2012 ist eine Privilege-Escalation-Schwachstelle bekannt, mit der Angreifer die Möglichkeit erhalten, sich mit Administrator-Rechten auf dem System und ggfs. in der Domäne zu bewegen.				
Empfehlung:	Die veraltete Software sollte entfernt (und ggfs. ersetzt) werden. Zusätzlich sollte das Patch-Management überprüft werden, ob sämtliche installierte Software hier aufgenommen ist.				
Referenzen:	https://news.microsoft.com/de-de/support-ende-windows-server-2008-und-sql-server-2008/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7253 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1761 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1762 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1763				

<div style="font-size: 48px; font-weight: bold; color: black;">M</div> <div style="font-size: 12px; font-weight: normal; color: black;">medium</div>	16. M – Microsoft Visual C++ Runtime veraltet		Elaborate	Complex	Simple
	Fehlerklasse: <i>Using Components with Known Vulnerabilities (OWASP A9)</i>	Grave			
		Serious		X	
		Light			
Betroffene Systeme:	<p>2005 Runtime: wviatqd001, wviatqw001, wviatqw002</p> <p>2008 Runtime: WOSIXQW007, WOSIXQW012, WOSIXQW013, WOSIXQW014, WOSIXQW015, WOSIXQW018, WOSIXQW020, WOSIXQW021 wviatqd001, wviatqw001, wviatqw002</p> <p>2010 Runtime: wviatqd001, wviatqw001, wviatqw002</p>				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	Auf den Servern sind veraltete Microsoft Runtime Libraries installiert.				
Auswirkung:	Die diversen Visual C++ Runtimes vor 2012 erhalten keine Sicherheitsupdates mehr. Für diese sind zahlreiche kritische Schwachstellen bekannt, bei den älteren beispielsweise Remote Code Execution Schwachstellen (besonders bei der GDI-Verarbeitung). Dadurch können Server ggfs. übernommen oder manipuliert werden.				
Empfehlung:	Die veraltete Software sollte entfernt (und ggfs. ersetzt) werden. Zusätzlich sollte das Patch-Management überprüft werden, ob sämtliche installierte Software hier enthalten ist.				
Referenzen:	https://docs.microsoft.com/de-DE/troubleshoot/cpp/minimum-service-pack-levels https://docs.microsoft.com/en-us/visualstudio/releases/2019/servicing-vs2019				

<div style="font-size: 48px; font-weight: bold; margin: 0;">M</div> <div style="font-size: 12px; font-weight: normal; margin-top: 5px;">medium</div>	17. M – Microsoft SQL-Server veraltet	Elaborate	Complex	Simple
	Fehlerklasse: <i>Using Components with Known Vulnerabilities (OWASP A9)</i>	Grave	Serious	Light
		Grave	Serious	Light
		Grave	Serious	Light
Betroffene Systeme:	wviaatqd001 wviaatqw001			
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.			
Sachverhalt:	Auf beiden Servern ist das Softwarepaket „Microsoft SQL Server 2008 Setup Support Files“ installiert. Der Support für SQL-Server 2008 endete vor 2 Jahren. Die Installation von SQL Server 2012 ist mit Version 11.2.5058.0 (07/2015) ebenfalls stark veraltet.			
Auswirkung:	Es konnte im Rahmen der Untersuchungen nicht festgestellt werden, ob SQL Server 2008 noch betrieben wird, oder nur Installationsreste gefunden wurden. Für SQL-Server 2008 sind Remote Code-Execution Schwachstellen bekannt. Für den SQL-Server 2012 ist eine Privilege-Escalation-Schwachstelle bekannt, mit der Angreifer die Möglichkeit erhalten, sich mit Administrator-Rechten auf dem System und ggfs. in der Domäne zu bewegen.			
Empfehlung:	Die veraltete Software sollte entfernt (und ggfs. ersetzt) werden. Zusätzlich sollte das Patch-Management überprüft werden, ob sämtliche installierte Software hier enthalten ist.			
Referenzen:	https://news.microsoft.com/de-de/support-ende-windows-server-2008-und-sql-server-2008/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7253 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1761 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1762 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1763			

<div style="font-size: 48px; font-weight: bold; margin: 0;">L</div> <div style="margin-top: 10px;">low</div>	18. L – Schwache Kryptographie für RDP und TLS		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse: <i>Sensitive Data Exposure</i> <i>(OWASP A3/A8)</i>	Serious	X		
		Light			
Betroffene Systeme:	10.59.143.77, 10.62.130.102, 10.62.130.103, 10.62.130.108, 10.62.43.78				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Bei verschiedenen eingesetzten Diensten ist die Konfiguration der verwendeten kryptografischen Absicherungsmaßnahmen unzureichend, so dass ein geringeres Schutzniveau erreicht wird, als dies eigentlich möglich wäre.</p> <p>Sowohl für Web-Anwendungen als auch RDP-Dienste werden schwache bis mittelstarke Chiffren eingesetzt, die nicht mehr dem Stand der Technik entsprechen und nicht mehr produktiv eingesetzt werden sollen:</p> <ul style="list-style-type: none"> - DES-CBC3-SHA (10.59.143.77:443, 10.62.130.102:3389, 10.62.130.103:443, 10.62.130.108:3389) <p>Auf den folgenden Diensten werden selbst-signierte SSL-Zertifikate verwendet, welche nicht von einer externen oder internen vertrauenswürdigen Zertifizierungsstelle ausgestellt wurden:</p> <ul style="list-style-type: none"> - 10.62.43.78:55087 (mssql), „Subject : CN=SSL_Self_Signed_Fallback“ - 10.62.130.102:3389 (rdp), „Subject : CN=WVIATQW001.fhhnet.stadt.hamburg.de“ - 10.62.130.108:3389 (rdp), „Subject : CN=WVIATQD001.fhhnet.stadt.hamburg.de“ <p>Auf mehreren Servern wird noch TLS 1.0 unterstützt. Das Protokoll bietet keine Unterstützung für moderne kryptografische Algorithmen und erfordern die Unterstützung des SHA1-Hashverfahren, das nicht mehr als sicher gilt. TLS 1.0 (sowie TLS 1.1) gelten seit März 2021 als „deprecated“ und werden vom BSI für den produktiven Einsatz nicht empfohlen. TLS 1.0 wird auf den folgenden Servern/Diensten unterstützt:</p> <ul style="list-style-type: none"> - 10.62.130.102:3389 (rdp) - 10.62.130.103:443 (https) - 10.62.130.108:3389 (rdp) <p>Auf zwei Systemen sind zudem noch RC4 Chiffren aktiv, welche bekannte Schwachstellen aufweisen und daher nicht mehr produktiv eingesetzt werden sollten. Die folgenden RC4 Chiffren wurden für die Dienste „10.62.130.102:3389 (rdp)“ und „10.62.130.103:443 (https)“ erkannt:</p> <ul style="list-style-type: none"> - RC4-MD5 - RC4-SHA 				

	Auch der Fernzugriff mittels des Remote-Desktop-Protokolls RDP ist in der untersuchten Umgebung nur unzureichend abgesichert. Im Test wurde festgestellt, dass die Authentisierung auf Netzwerkebene (Network Level Authentication, NLA) nicht aktiviert ist.
Auswirkung:	Die eingesetzten Verschlüsselungsprotokolle bieten ein geringeres Schutzniveau als der aktuelle Stand der Technik. Teilweise sind Angriffe mit überschaubarem Ressourceneinsatz möglich. Die Vertraulichkeit und Integrität der übertragenen Daten sowie die Absicherung vor Man-in-the-Middle-Angriffen, die aktiv in geschützte Verbindungen eingreifen, wird dadurch gefährdet.
Empfehlung:	Entwerfen Sie ein Kryptokonzept, welches die Mindestanforderungen an einzusetzende kryptografische Algorithmen protokollunabhängig festhält. Dieses Konzept sollte beispielsweise Mindestschlüssellängen für asymmetrische und symmetrische Verschlüsselungsalgorithmen sowie einzusetzende Hashing- und Signaturverfahren enthalten. Prüfen sie anschließend für die Konfiguration vorhandener Dienste, die kryptografische Algorithmen verwenden, ob diese dem Kryptokonzept entsprechen. Dabei sollten zumindest die Dienste mit SSL/TLS sowie RDP betrachtet werden.
Referenzen:	http://www.rapid7.com/db/vulnerabilities/ssl2-and-up-enabled http://technet.microsoft.com/de-de/library/cc770833.aspx http://technet.microsoft.com/de-de/library/cc732713.aspx https://www.ssllabs.com/projects/best-practices/

<div style="font-size: 48px; font-weight: bold; margin: 0;">L</div> <div style="font-weight: bold; margin-top: 10px;">low</div>	19. L – Hohe Systemlast auf Servern		Elaborate	Complex	Simple
	<i>Fehlerklasse: Ungeeignete Sicherheitsarchitektur</i>				
			x		
Betroffene Systeme:	(von Administratoren nicht genauer benannt)				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Bei nachträglichen Prüfungen konnte festgestellt werden, dass ein auf Default-Einstellungen parametrisierter Portscan mit NMAP auf den Servern für hohe Systemlast sorgte, die diese zwar nicht vollständig unbenutzbar machte, aber merklich negativ beeinflusste.</p> <p>Den Berichten eines Administrators zufolge sorgte die installierte "McAfee Endpoint Security (ENS) 10.7.0" beim Scan für massive Systemlast.</p>				

Auswirkung:	Die Systeme können durch einen einfachen Port-&Servicescan (Nessus in Default-Einstellung) stark belastet und ggfs. sogar praktisch kaum noch nutzbar werden.
Empfehlung:	Es sollte zusammen mit dem Hersteller untersucht werden, wie eine starke Systembelastung zustande kommt und wie die Auswirkungen verringert werden können.

<div style="font-size: 48px; font-weight: bold; margin: 0;">L</div> <div style="margin-top: 10px;">low</div>	20. L – Microsoft Silverlight installiert		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse: <i>Using Components with Known Vulnerabilities (OWASP A9)</i>	Serious	x		
		Light			
Betroffene Systeme:	OSI-Plattform: WOSIXQW007, WOSIXQW012, WOSIXQW013, WOSIXQW014, WOSIXQW015, WOSIXQW018, WOSIXQW020, WOSIXQW021 ViatoZ-Server: wviatqd001, wviatqw001, wviatqw002				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	Auf den Servern ist das das IE-Plugin „Silverlight“ installiert, dessen Supportende erreicht ist.				
Auswirkung:	Die Software wird nicht mehr mit Sicherheitsupdates versorgt. Aktuell sind keine schwerwiegenden Sicherheitslücken bekannt und da diese Software üblicherweise keine Serverkomponente zur Verfügung stellt, ist das unmittelbare Risiko für den Serverbetrieb eher gering einzustufen.				
Empfehlung:	Die veraltete Software sollte aktualisiert oder entfernt werden. Zusätzlich sollte das Patch-Management überprüft werden, ob sämtliche installierte Software hier enthalten ist.				
Referenzen:	https://support.microsoft.com/de-de/windows/supportende-f%C3%BCr-silverlight-0a3be3c7-bead-e203-2dfd-74f0a64f1788				

<div style="font-size: 2em; font-weight: bold; margin-bottom: 5px;">I</div> <div style="font-size: 0.8em;">info</div>	21. I – Härten ohne Herleitung		Elaborate	Complex	Simple
		Grave			
	Fehlerklasse:	Wählen Sie ein Element aus.	Serious		
			Light		
Betroffene Systeme:	Alle Windows-Systeme				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>GPOs: Härten sind umfangreich vorhanden, aber nicht immer sicherheitsoptimiert (NTLMv2 erlaubt, Files WxX fehlt, lokale Firewalls erlauben „any“ Quellen für die jeweils installierten Dienste).</p> <p>Aufgrund fehlender Hintergründe zu den jeweiligen Entscheidungen sind die verteilten GPOs aber nicht wirklich bewertbar.</p>				

8 KONFIG-AUDIT FIREWALLS

Die Sichtprüfung von Firewallregeln wurde am 19.06.2021 in einer Videokonferenz mit Herrn Horstmann durchgeführt.

8.1 Geprüfte Firewallkonfigurationen

Dataport nutzt NetSPoC (Network Security Policy Compiler <https://hknutzen.github.io/Netspoc/>) zur zentralen Konfiguration seiner Firewalls.

NetSPoC prüft laut Interviewaussage auf "overlaps" (Masking), so dass übergreifende/maskierende Regeln nicht implementierbar sind.

In Richtung Internet werden Barracuda CloudGen Firewalls IVZ eingesetzt, ansonsten Cisco ASA. Der vorgelegten Verbundsdefinition nach ist der Firewall-Betrieb von der Zertifizierung nach ISO-27001 umfasst.

8.2 Einschränkungen

Da weder eine vollständige Kommunikationsmatrix noch Kommunikationspfade vorgelegt werden konnten, war weder eine Konfigurationsprüfung der beteiligten (weil nicht identifizierbaren) Firewalls möglich, noch eine Überprüfung auf Zugriffe von anderen Netzen oder zu anderen Zwecken.

Mangels Netz- bzw. Systemübersicht konnte zudem nicht verifiziert werden, in welche Systeme sich mit dem Fachverfahren im selben Netz befanden, welche Basis- oder Mehrverfahrensdienste Zugriff haben.

Mangels belastbarer Architektur- oder Systembeschreibung der OSI-Plattform kann keine Einschätzung zu eventuell möglichen Zugriffen durch andere Verfahren oder Systeme dort getroffen werden.

Dass während der Prüfungen keine Regeln für den später identifizierten Mehr-Verfahrens-Dienst (MVD) FileTransfer auftauchten, legt nahe, dass es übergreifende Firewall-Regeln geben muss - die aber nicht gezeigt wurden.

8.3 Vorgehen

In den Konfigurationsdateien des Firewall-Management-Tools wurde nach IP-Adressen oder Namen der ViatoZ-Server gesucht und die entsprechenden Regeln vom Administrator kurz präsentiert und in Augenschein genommen.

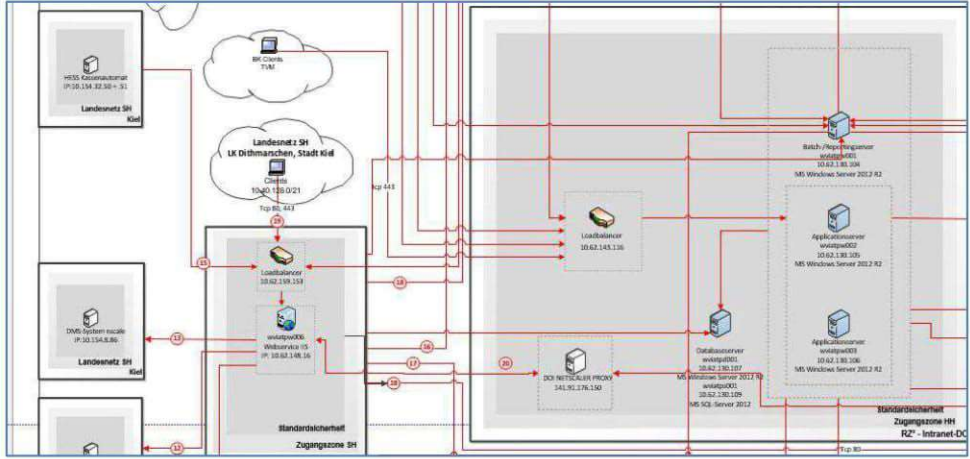
Konfigurationsdateien wurden auch auf Anfrage nicht zur Verfügung gestellt.

8.4 Ergebnisse

Aus der Prüfung ergaben sich folgende Befunde:

<h1 style="font-size: 48px; margin: 0;">H</h1> <p style="font-weight: bold; margin: 5px 0;">high</p>	22. H – Widersprüchliche Aussagen zur Firewall-Existenz		Elaborate	Complex	Simple
	Fehlerklasse: <i>Security Misconfiguration (OWASP A6)</i>	Grave		X	
		Serious			
		Light			
Betroffene Systeme:	OSI-Plattform				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Laut Firewall-Admin stehen zwischen den OSI SC App-Servern (VLAN 254) und den OSI BackendWS (VLAN 354) keine Firewalls (mittlerer Block). In VLANs 254 + 354 befänden sich laut Admin zwar nur OSI-Server, aber nicht nur für i-KFZ, sondern für einige hundert nicht beteiligte Fachverfahren.</p> <p>Ebenso wenig existierten laut dessen Aussage Firewalls zwischen OSI BackendWS und den ViatoZ-Systemen (im folgenden Architekturbild mitte oben nach rechts unten), da diese in derselben Zugangs- und Sicherheitszone liegen.</p>				
	<p>Das Fehlen von Firewalls wird von OSI-Betreuern bestritten. Genauere Dokumentation konnte aber von keiner Seite vorgelegt werden.</p>				
Auswirkung:	<p>Die Systeme haben ggfs. mehr Zugriffsmöglichkeiten als in den KBA-Mindestanforderungen vorgesehen.</p> <p>Auch sind offenbar nicht alle Kommunikationsbeziehungen bekannt oder kommuniziert, was eine Risikoeinstufung und auch die Betriebssicherheit gefährdet.</p>				
Empfehlung:	<p>Sämtliche verwendeten Kommunikationsbeziehungen müssen identifiziert (ggfs. reverse-engineert) und dokumentiert werden.</p>				

In Zusammenhang mit den Mindestanforderungen des KBA ist zu prüfen, ob die jeweiligen Freischaltungen zulässig sind.

<h1 style="font-size: 48px; margin: 0;">M</h1> <p style="font-weight: bold; margin-top: 10px;">medium</p>	<h3>23. M – Fehlende Mandantentrennung</h3>		Elaborate	Complex	Simple
	<p>Fehlerklasse: <i>Ungeeignete Sicherheitsarchitektur</i></p>	Grave			
		Serious		X	
		Light			
<p>Betroffene Systeme:</p>	ViatoZ-Server				
<p>Nachtest:</p>	Ein Nachtest wurde noch nicht durchgeführt.				
<p>Sachverhalt:</p>	<p>Das Produktions- und QS-System liegen im selben Netz, können entsprechend ungefiltert aufeinander zugreifen.</p>  <p>Zudem verwenden die beiden Mandanten Kiel/Schleswig-Holstein und Hamburg denselben Batch&Reporting-Server und denselben Datenbankserver.</p>				
<p>Auswirkung:</p>	<p>Die in den Mindestvoraussetzungen des KBA vorgeschriebene Mandantentrennung wird auf Serverebene nicht erreicht. Das System ist dadurch nicht zulässig.</p> <p>Durch die fehlende netzwerkseitige Trennung zwischen Test- und QS-Systemen könnten Fehlkonfigurationen zu verlorenen (wenn Prod in QS schreibt) oder fehlerhaften (wenn QS in Prod schreibt) Mitteilungen gegenüber dem KBA führen.</p>				

Empfehlung:	<p>QS- und Produktiv-Umgebungen sollten auch netzwerktechnisch strikt voneinander getrennt betrieben werden.</p> <p>Für unterschiedliche Mandanten sind nach KBA-Vorgabe auch unterschiedliche Server zu betreiben. Entsprechend müssen hier jeweils dedizierte Systeme aufgebaut werden.</p>
-------------	---

<h1 style="font-size: 48px; margin: 0;">M</h1> <p style="font-weight: bold; margin: 5px 0 0 0;">medium</p>	<p>24. M – Server wenig abgeschirmt</p>		Elaborate	Complex	Simple
	<p>Fehlerklasse: <i>Security Misconfiguration (OWASP A6)</i></p>	Grav e	X		
		Serious			
		Light			
Betroffene Systeme:	ViatoZ-Server				
Nachtest:	Ein Nachtest wurde noch nicht durchgeführt.				
Sachverhalt:	<p>Die Server des Fachverfahrens können über den Proxy direkt auf das Internet zugreifen.</p> <p>Da die Server in Netzen der "Standardsicherheit" positioniert sind (laut Admin also für Server mit geringerem Sicherheitsbedarf) ist der Zugriff in Richtung Internet nicht weiter eingeschränkt.</p>				

```
service:DOI_NETSCALER_PROXY_HH = {  
  description = ausgehende Verbindungen vom Netscaler zum DOI Proxy 141.91.176.150 (Thiess)  
  
  user = interface:d30-alg010-hh.ALG_BI-NETZMANAGEMENT_NOB-NETZ_PROD_HH_10_62_143_138,  
        host:wviafpw001_10_62_130_10,  
        host:wviafqw001_10_62_130_11,  
        host:wviafqw002_10_62_130_12,  
        host:wviafpw002_10_62_130_13,  
        host:wviafpw003_10_62_130_14,  
        host:wviatqw001_10_62_130_102,  
        host:wviatqw002_10_62_130_103,  
        host:wviatpw001_10_62_130_104,  
        host:wviatpw002_10_62_130_105,  
        host:wviatpw003_10_62_130_106,  
        ;  
  permit src = user;  
        dst = host:LNHH_141_91_176_150;  
        prt = tcp 80;  
}
```

.10-.14 für Führerscheinesen ViatoF - jeweils incl. QS (10+11 im Abbau)
.102-.106 ViatoZ Zulassung - jeweils incl. QS

Laut Fachbereich wird der Internetzugriff für den Zugriff auf TÜV, DEKRA, ... und Gutachten benötigt. Diese Anforderung findet sich aber nicht im gestellten Freischaltungsantrag.

Auswirkung:	Die Systeme haben mehr Zugriffswege als in den KBA-Mindestanforderungen vorgesehen. Auch sind offenbar nicht alle Kommunikationsbeziehungen bekannt oder kommuniziert, was eine Risikoeinstufung und auch die Betriebssicherheit gefährdet.
Empfehlung:	Sämtliche verwendeten Kommunikationsbeziehungen müssen identifiziert (ggfs. reverse-engineert) und dokumentiert werden. In Zusammenhang mit den Mindestanforderungen des KBA ist zu prüfen, ob die jeweiligen Freischaltungen zulässig sind.

ANHANG A BERÜCKSICHTIGUNG DER OWASP TOP TEN

Die Untersuchung der Web-Oberflächen berücksichtigte die in den „OWASP Top Ten 2017“ veröffentlichten typischen Fehler, blieb aber nicht auf diese beschränkt.

Tabelle 11: OWASP-Top-Ten-Checkliste

Angriff	Beschreibung	Geprüft
A1 Injection	Es wurde getestet, ob durch Einfügen von Sonderzeichen Kommandos in Eingabedaten eingefügt werden können. Getestet wurde (sofern notwendig): <ul style="list-style-type: none">• SQL Injection• LDAP Injection• ORM Injection• XML Injection• SSI Injection• XPath Injection• IMAP/SMTP Injection• Code Injection• OS Command Injection• Buffer overflow	Ja
A2 Broken Authentication and Session Management	Das Session Management der Web-Anwendung wurde daraufhin untersucht, ob einer der folgenden Angriffe möglich ist: <ul style="list-style-type: none">• User Enumeration• Guessable User Account (15 beliebte Passwörter)• Brute Force Testing (nur soweit vereinbart)• Vulnerable remember password and password reset• Bypassing authentication schema• Logout and Browser Cache Management• Use and quality of CAPTCHA• Multiple Factors Authentication (sofern vorhanden)• Race Conditions• Session Management Schema• Cookie Attributes• Session Fixation• Exposed Session Variables• CSRF (as the target)• Privilege Escalation	Ja

Angriff	Beschreibung	Geprüft
A3 Sensitive Data Exposure	<p>Die auf der Website eingesetzte Verschlüsselung der Verbindungen wurde auf die Qualität der Algorithmen und Zertifikate hin untersucht.</p> <p>Ob Passwörter und andere sensible Daten nur über eine verschlüsselte Verbindung transportiert werden, ist bereits Teil der Prüfungen unter A2.</p> <p>Eine Prüfung von kryptografisch gesicherter serverseitiger Datenhaltung kann nur in einem Code- oder Config-Review erfolgen.</p>	Ja
A4 XML External Entities (XXE)	<p>Es wurde überprüft, ob die Anwendung einen anfälligen XML Verarbeiter einsetzt, der externe Entitäten verarbeitet. Es wurde getestet, ob eigener XML Code hochgeladen oder von anderen Stellen eingebunden werden kann oder ob vom Nutzer beeinflussbarer Inhalt in XML Dokumente eingebunden wird. Zudem wurde geprüft, ob durch manipuliertes XML ein Fehler im Parser hervorgerufen werden kann.</p>	Ja
A5 Broken Access Control	<p>Es wurde getestet, ob auf bestimmte Daten direkt zugegriffen werden kann. Es wurde überprüft, ob durch Änderungen an Parametern andere Daten direkt geändert werden können.</p> <p>Es wurde versucht, direkt auf URLs und Funktionalitäten zuzugreifen ohne vorher alle normalerweise dafür notwendigen Schritte zu durchlaufen.</p>	Ja
A6 Security Misconfiguration	<p>Die Web-Anwendung wurde daraufhin untersucht, ob einer der folgenden Angriffe möglich ist:</p> <ul style="list-style-type: none"> • Objects with special content (z.B. info.php) • Revealing Error Codes and Messages • Erroneous File Extension Handling • Dangerous HTTP Methods and XST (Cross Site Tracing) 	Ja
A7 Cross-Site Scripting (XSS)	<p>Es wurde getestet, ob durch Einfügen von Sonderzeichen Cross-Site-Scripts in die Anfrage eingefügt werden können. Getestet wurde (sofern notwendig):</p> <ul style="list-style-type: none"> • Reflected Cross Site Scripting • Stored Cross Site Scripting • DOM-based Cross Site Scripting • Cross Site Flashing 	Ja
A8 Insecure Deserialization	<p>Es wurde überprüft ob serialisierte Daten an den Server geschickt werden. Wenn dies der Fall war, wurde versucht über gezielte Veränderungen an dem serialisierten Objekt eine Änderung im Verhalten des Servers auszulösen.</p>	Ja

Angriff	Beschreibung	Geprüft
A9 Using Components with Known Vulnerabilities	Es wurde, soweit möglich, getestet, ob Software oder Komponenten eingesetzt werden, die bekannte Schwachstellen aufweisen. Eine eingehende Prüfung kann nur in einem Code- oder Config-Review erfolgen.	Ja
A10 Insufficient Logging&Monitoring	In den meisten Black-Box Penetrationstests kann nicht überprüft werden, ob ein ausreichendes Logging und Monitoring stattfindet. Bei der Prüfung wird in der Regel im Nachgang des Penetrationstests überprüft, ob zu allen relevanten Aktionen entsprechende Logeinträge vorhanden sind. Eine eingehende Prüfung diesbezüglich kann nur in Absprache mit dem Auftraggeber erfolgen.	Nein

A.1 Fehlerklassen

Die HiSolutions AG verwendet Fehlerklassen für die Einteilung der Befunde. Die Fehlerklassen sind abgeleitet von den OWASP Top Ten, bilden darüber hinaus aber auch weitere Befundtypen ab.

Server-side Injection (OWASP A1)	Serverseitige Injection-Schwachstellen
Broken Authentication & Session Mgmt. (OWASP A2)	Schwachstellen in der Nutzerverwaltung und -authentisierung
Sensitive Data Exposure (OWASP A3)	Schwachstellen durch eine mangelhafte Verschlüsselung insbesondere bei der Übertragung
XML External Entities (OWASP A4)	Schwachstellen in der XML Verarbeitung
Broken Access Control (OWASP A5)	Schwachstellen, die einen direkten Zugriff auf Ressourcen erlauben oder durch mangelnde Rechtekontrolle entstehen
Security Misconfiguration (OWASP A6)	Schwachstellen durch eine unsichere Konfiguration
Client-side Injection (OWASP A7)	Clientseitige Injection-Schwachstellen
Insecure Deserialization (OWASP A8)	Schwachstellen, die durch unsicheres deserialisieren von Daten entstehen
Using Components with Known Vulnerabilities (OWASP A9)	Schwachstellen durch Einsatz von veralteten oder unsicheren Komponenten
Insufficient Logging & Monitoring (OWASP A10)	Fehlerhaftes Logging und Monitoring der Systeme und Anwendungen
Anwendung: Design-Fehler	Fehler im grundlegenden Design der Anwendung (nicht von den OWASP Top Ten abgebildet)
Anwendung: Implementierungs-Fehler	Implementierungsfehler in der Anwendung (nicht von den OWASP Top Ten abgebildet)
Ungeeignete Sicherheitsarchitektur	Schwachstellen in der grundlegenden Architektur (nicht von den OWASP Top Ten abgebildet)
Mangelnde Systempflege	Schwachstellen, die durch „vergessene“ Dienste und Systeme entstehen (nicht von den OWASP Top Ten abgebildet)
Info/Funktionalität	Weitere Befunde ohne Sicherheitsbezug

ANHANG B EMPFEHLUNGEN ZU HÄUFIGEN FEHLERKLASSEN

Die folgenden Fehlerklassen treten in Sicherheitstests sehr häufig auf und wurden auch im vorliegenden Test identifiziert. Sie werden hier mit entsprechenden Empfehlungen zur Vermeidung ausführlich vorgestellt.

B.1 Cross-Site-Scripting (XSS)

Beim Cross-Site-Scripting werden durch einen Angreifer Teile der ursprünglichen Seite durch gefälschten HTML- oder JavaScript-Code ausgetauscht. Dies erfolgt nicht durch eine Veränderung des durch den Server bereitgestellten Webauftrittes, sondern in speziell präparierten Links oder HTML-E-Mails, die potentiellen Opfern untergeschoben werden. Dies kann im einfachsten Fall für Phishing-Angriffe missbraucht werden, um beispielsweise Anmeldeinformationen zu stehlen.

Grundsätzlich ist es durch XSS möglich, den gesamten Inhalt der angegriffenen Website nach Vorstellung des Angreifers zu verändern. In der Praxis wird XSS vorrangig zum Übernehmen von authentifizierten, gültigen Websitzungen (Sessions), zum Stehlen von Authentifizierungsdaten oder Benutzerinformationen verwendet.

Bei XSS kann zwischen nicht-persistentem und persistentem XSS unterschieden werden: Während bei ersterem eine präparierte URL zum Einschleusen des Fremdcodes verwendet wird, kann bei zweitem der modifizierende Code permanent in einer Datenbank auf dem Server (z. B. in Gästebüchern oder Foren) gespeichert werden. Dies ist für Angreifer die attraktivere Variante, da der sonst notwendige Schritt ausbleiben kann, Opfern die modifizierte URL unterzuschieben. Persistentes XSS würde somit bei jedem Betrachten durch den Browser des Betrachters ausgeführt werden.

Der Nachweis von XSS-Schwachstellen wird üblicherweise durch Einschleusen von Code-Fragmenten, etwa in der Form `<script>alert('XSS');</script>`, geführt.

Ist eine Schwachstelle vorhanden, wird der eingeschleuste Code ausgeführt. Die Website selbst wird bei diesem Test jedoch ansonsten nicht modifiziert. Bei einem realistischen Angriff würde ein Angreifer allerdings komplexeren Code unterschieben, der dazu geeignet ist, das erwünschte Ziel zu erreichen. Dabei ist es auch möglich, den Benutzer auf fremde Server unter der Kontrolle des Angreifers umzuleiten oder Code nachzuladen.

Weiterführende Erklärungen und allgemeine Beispiele finden Sie unter:

- http://www.owasp.org/index.php/Cross-site_scripting
- <http://hackers.org/xss.html>

Wir empfehlen die Implementierung eines Defense-in-Depth-Ansatzes wie nachfolgend dargestellt.

B.1.1 Durchgängige Implementierung einer Ausgabecodierung

Neben der Eingabvalidierung muss immer eine Ausgabecodierung stattfinden. Eine korrekte Ausgabecodierung stellt sicher, dass die betreffenden Daten nicht als Befehle ausgeführt, sondern passend dargestellt oder anderweitig verarbeitet werden. Dabei müssen in Abhängigkeit der Ausgabeschnittstelle bzw. der Zieltechnologie bestimmte Konversionsfilter eingesetzt werden („Escaping“). Bei einer Ausgabe in HTML etwa sollte eine HTML-Codierung stattfinden, in JavaScript-Zeichenketten ist das Hex-Encoding (`\xHH`, für Unicode `\uHHHH`) zu verwenden.

In manchen Zusammenhängen, z. B. JavaScript außerhalb von „gequoteten“ Zeichenketten, ist eine sichere Kodierung nicht wirklich zuverlässig möglich. Unterschiede zwischen Browsern und Browser-Versionen, die Verschachtelung von Kontexten, etwa URL in JavaScript in HTML Event Handlern, sowie Technologie-Änderungen und Weiterentwicklungen machen es unmöglich, allgemeingültige Regeln für eine sichere Ausgabecodierung festzulegen. Von Nutzern stammende Daten sollten daher nur an einigen „sicheren“ Positionen in einer HTML-Seite eingefügt werden. Diese Positionen sind durch die Regeln 1 bis 5 in dem Dokument

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
[https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

gegeben. Eine Kurzfassung aller Regeln findet sich im gleichen Text, unter

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html#xss-prevention-rules-summary.

Eine Ausnahme für diese Regeln stellen Situationen dar, in denen ein Eingabefilter sicherstellt, dass die betreffenden Daten nur aus alphanumerischen Zeichen bestehen, also jede Art von Sonderzeichen ausgeschlossen wird.

Werden die eingegebenen Daten nicht direkt vom Webserver in die Seite eingefügt, sondern dynamisch per JavaScript in die DOM-Darstellung des HTML-Codes geschrieben (via `document.write()` oder ähnlichen Funktionen), so werden XSS-Angriffe, aber auch der Schutz vor diesen, um einiges komplexer. Man spricht in diesem Fall von „DOM-basierten XSS-Angriffen“. Um diese Attacken auszuschließen, sollte den Empfehlungen in

https://cheatsheetseries.owasp.org/cheatsheets/DOM_based_XSS_Prevention_Cheat_Sheet.html gefolgt werden.

B.1.2 Einschränkung der Auswirkungen von XSS

Der häufigste Einsatz von XSS besteht im Diebstahl von Session-Cookies, so dass der Angreifer den Login eines Nutzers übernehmen kann. Um den Session-Cookie auslesen zu können, nutzt der Angreifer JavaScript.

Es ist möglich, das Auslesen des Session-Cookies und die Übernahme der Session durch flankierende Maßnahmen zu verhindern, so dass selbst bei Vorhandensein eines XSS-Fehlers kaum Schaden entsteht:

- Das Auslesen des Session-Cookies durch JavaScript kann durch das Setzen des Flags „HttpOnly“ verhindert werden.
- Alle Webseiten innerhalb des Scopes des Cookies können den Cookie potenziell auslesen. Der „Scope“ des Cookie sollte daher möglichst klein gewählt werden („path“-Flag). Für Session-Cookies sollte der Scope praktisch immer auf einen Server beschränkt bleiben.
- Wird der Cookie nur über HTTPS benutzt, sollte zusätzlich das „secure“-Flag gesetzt werden; damit kann der Cookie nicht mehr unverschlüsselt übertragen werden.
- Die TRACE/TRACK-Option des Webserver muss deaktiviert sein; sie erlaubt die Umgehung des HttpOnly-Flags.

B.1.3 Implementierung einer Eingabevalidierung auf Serverseite

Zur serverseitigen Eingabevalidierung sollte nach Möglichkeit eine Whitelist-Prüfung implementiert werden, die nur solche Inhalte akzeptiert, die als sinnvolle Eingaben in Frage kommen (nur Ziffern, gültige E-Mail-Adressen usw.). Wird eine Eingabe nicht akzeptiert, so sollte sie in Gänze zurückgewiesen werden, anstatt z. B. einzelne Zeichen zu löschen oder zu ersetzen.

Nicht empfehlenswert ist der Versuch, aus Eingaben einzelne Zeichenketten wie `<script>` herauszufiltern. Derartige Filter können praktisch nie einen vollständigen Schutz gewährleisten, da nur einfachste Angriffsarten abgefangen werden.

Entwicklungsframeworks wie J2EE, .NET oder ASP bieten bereits geeignete Validierungsmethoden, die nach Möglichkeit eingesetzt werden sollten.

Die Eingabevalidierung alleine bietet allerdings keinen Schutz gegen XSS – nur bei sehr begrenzten Input-Formaten (z. B. Auswahllisten, Integer-Zahlen) kann dies gesichert werden. Sie erschwert

jedoch bei vielen Werten generell eine Injektion und hilft, Logik-Fehlern durch unerwartete Inhalte vorzubeugen.

B.1.4 Content Security Policy

Der W3-Standard „Content Security Policy“ definiert zusätzliche Einschränkungen für die Ausführung von aktiven Inhalten, die die klassische Same Origin Policy erweitern. Diese Restriktionen werden über den HTTP-Header Content-Security-Policy gesetzt und beschränken die Quellen, aus denen der Webbrowser JavaScript, aber auch Flash- und Java-Applets sowie weitere nachladbare Dateien akzeptiert. Abhängig vom Browsertyp muss alternativ der Header X-Content-Security-Policy oder X-WebKit-CSP verwendet werden. Am sinnvollsten ist es, alle drei Header gleichzeitig zu setzen, um alle gängigen Browser abzudecken.

Erkennt der Webbrowser den Header, so wird unter anderem die Ausführung von Skripten, die in der Seite eingebettet sind, sowie die dynamische Auswertung von Code mittels Funktionen wie eval() verhindert. Allein dies genügt, um eine große Klasse von XSS-Angriffen unwirksam zu machen, erfordert jedoch einige Anpassungen des Aufbaus bestehender Seiten. Der Content-Security-Policy-Header kann zusätzliche Direktiven enthalten, die eine feinere Anpassung der verschiedenen Beschränkungen ermöglicht.

Trotz der zu leistenden Anpassungen bei älteren Webanwendungen ist das Setzen der Content Security Policy ein erheblicher Sicherheitsgewinn, für Neuentwicklungen sollte die Nutzung dieses Standards auf jeden Fall eingeplant werden.

Eine Übersicht der Spezifikation findet sich in

<http://www.heise.de/security/artikel/XSS-Bremse-Content-Security-Policy-1888522.html?view=print>,

der Standard selbst ist auf <http://www.w3.org/TR/CSP/> veröffentlicht.

B.2 Patch-Management

Ein nicht funktionierendes Patch-Management ist eine der häufigsten Problemquellen. Ein geregelter Patch-Management-Prozess umfasst alle eingesetzten Systeme und Komponenten und beinhaltet die folgenden Teilschritte:

Tabelle 12: Schritte im Patch-Management-Prozess

Teilschritt	Beschreibung
Patch-Beschaffung	Es sind Informationswege eingerichtet, auf denen die Systemverantwortlichen über neue Schwachstellen oder Sicherheitsupdates, die ihr System betreffen, informiert werden. Die Systemverantwortlichen beziehen Updates auf einem vertrauenswürdigen, manipulationssicheren Kanal.
Patch-Prüfung	Es ist darauf zu achten, dass Patches und Updates wie jede andere Software nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Es ist wichtig, dass Integrität und Authentizität der für die bereits installierten Produkte einzuspielenden Sicherheitsupdates und Patches überprüft werden.
Beantragung der Patch-Installation	Die Beantragung der Installation oder des Einspielens von Patches auf das entsprechende System erfolgt über den Change-Management-Prozess. Sollte es erforderlich sein, dass Patches beispielsweise wegen gefährlicher Sicherheitslücken umgehend eingespielt werden müssen, so sind sie wie dringliche Changes zu behandeln.
Patch-Test	Sicherheitsupdates oder Patches dürfen jedoch nicht voreilig auf die Systeme eingespielt werden, sondern müssen vor dem Einspielen getestet werden. Die

Tests erfolgen im Rahmen des Change-Management-Prozesses und sind in einer Testumgebung durchzuführen.

Datensicherung der IT-Systeme	Vor der Installation eines Updates oder Patches wird stets eine Datensicherung des betroffenen Systems erstellt, um in der Lage zu sein, beim Fehlschlagen der Installation den Originalzustand wieder herzustellen.
Planung der Installation	Die Planung der Installation erfolgt im Rahmen einer Planung zur Durchführung von Changes, unterliegt den Anforderungen der Priorisierung und Ressourcenverfügbarkeit und ist in den Änderungskalender aufzunehmen.
Patch-Installation	Die Installation ist durch das Change Management zu koordinieren und wird durch die entsprechenden Systemverantwortlichen durchgeführt.
Dokumentation	Die Dokumentation einer Patch-Installation entspricht der Dokumentation eines Changes, d. h. es sind der Anlass, von wem und wann die Installation durchgeführt wurde, zu dokumentieren. Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit ermitteln lassen, um beim Bekanntwerden von Schwachstellen schnell Klarheit darüber zu erhalten, ob das System gefährdet ist. Die Änderungen sind in den Change Log aufzunehmen, und die relevante Systemdokumentation muss aktualisiert werden.
Rollout	Sollte eine ganze Umgebung aktualisiert werden, so kann die Installation im Rahmen eines Releases durchgeführt werden. Dieses kann in Stufen eingeteilt werden, wobei die erste Stufe die am wenigsten kritischen Systeme beinhaltet.

ANHANG C BEWERTUNGSSKALEN FÜR SCHWACHSTELLEN

Tabelle 13: Komplexitätsskala

Komplexität	Definition
Elaborate	Die Schwachstelle ist sehr schwer auszunutzen, weil <ul style="list-style-type: none">– ein Exploit selbst entwickelt werden muss,– die Ausnutzung nur unter speziellen Bedingungen möglich ist,– nur ein sehr kleiner Kreis von Personen in Frage kommt oder– ein komplexer Umweg wie z. B. ein gezielter Phishing-Angriff notwendig ist
Complex	Die Schwachstelle ist schwer auszunutzen, weil <ul style="list-style-type: none">– ein Exploit selbst entwickelt oder angepasst werden muss,– hohe Kompetenz notwendig ist oder– ein komplexer Umweg wie z. B. ein weit gestreuter Phishing-Angriff notwendig ist
Simple	Die Schwachstelle ist einfach auszunutzen, weil <ul style="list-style-type: none">– ein Exploit verfügbar ist,– wenig Kompetenz nötig ist oder– kein Umweg notwendig ist.

Tabelle 14: Auswirkungsskala

Auswirkung	Definition
Grave	<p>Vertraulichkeit und Integrität, betreffend</p> <ul style="list-style-type: none">– eine große Menge an nicht für die Öffentlichkeit bestimmten Daten, oder– eine nicht geringfügige Menge an Daten, die vom BDSG besonders geschützt sind– im lesenden oder schreibenden Zugriff <p>Verfügbarkeit:</p> <ul style="list-style-type: none">– Eine Störung über mehrere Tage erscheint möglich
Serious	<p>Vertraulichkeit und Integrität:</p> <ul style="list-style-type: none">– erhebliche Menge an nicht für die Öffentlichkeit bestimmten Daten, die nicht vom BDSG besonders geschützt sind, oder– eine geringfügige Menge vom BDSG geschützter Daten– im lesenden oder schreibenden Zugriff <p>Verfügbarkeit:</p> <ul style="list-style-type: none">– Eine Störung über mehrere Stunden erscheint möglich
Light	<p>Vertraulichkeit und Integrität:</p> <ul style="list-style-type: none">– nur wenige oder halböffentliche Daten, die nicht vom BDSG geschützt sind,– im lesenden Zugriff <p>Verfügbarkeit:</p> <ul style="list-style-type: none">– Es erscheint eine nur kurze Störung möglich

ANHANG D SCHWACHSTELLENVERZEICHNIS

1.	H – Ungeeignete Integration der i-Kfz-Systeme in die zentrale OSI-Plattform	18
2.	H – Unzureichende Beachtung der KBA-Mindestanforderungen bei der Planung und Wartung der Umgebung	19
3.	H – Unvollständige interne Übersicht über i-Kfz Komponenten	20
4.	H – Mangelhafte zentrale Übersicht über notwendige oder erlaubte i-Kfz- Kommunikationsverbindungen	21
5.	H – Mangelhafte Umsetzung der i-Kfz-Netzbereiche	22
6.	H – Teilweise keine Verwendung und Umsetzung der geforderten i-Kfz-Schnittstellen	24
7.	H – Schnittstelle C mit Fremd-Administratoreingriff	26
8.	M – Zugriffsweg und Absicherung Schnittstelle D unbekannt	28
9.	OK – Keine unnötige Angriffsfläche	31
10.	M – Ungenügender Schutz vor Cross-Site-Scripting (XSS) Angriffen	34
11.	L – Detaillierte Fehlermeldungen geben interne Details preis	37
12.	L – Verbesserungswürdiger Schutz von Cookies	41
13.	L – Einsatz veralteter JavaScript Bibliotheken	43
14.	H – Kritisch veralteter McAfee-Agent	48
15.	M – Microsoft SQL-Server veraltet	49
16.	M – Microsoft Visual C++ Runtime veraltet	50
17.	M – Microsoft SQL-Server veraltet	51
18.	L – Schwache Kryptographie für RDP und TLS	52
19.	L – Hohe Systemlast auf Servern	53
20.	L – Microsoft Silverlight installiert	54
21.	I – Härtungen ohne Herleitung	55
22.	H – Widersprüchliche Aussagen zur Firewall-Existenz	57
23.	M – Fehlende Mandantentrennung	58
24.	M – Server wenig abgeschirmt	59

KONTAKT

██████████

Fon +49 30 533289-0

██████████@hisolutions.com

HiSolutions AG

Schloßstraße 1

12163 Berlin

info@hisolutions.com

www.hisolutions.com

Fon +49 30 533 289-0

Fax +49 30 533 289-900

Niederlassung

Frankfurt am Main

Mainzer Landstraße 50
60325 Frankfurt am Main

Fon +49 30 533 289 0

Fax +49 30 533 289 900

Niederlassung

Bonn

Heinrich-Brüning-Straße 9
53113 Bonn

Fon +49 228 52 268 175

Fax +49 30 533 289 900

Niederlassung

Düsseldorf

Kaiserwerther Str. 135
40474 Düsseldorf

Fon +49 30 533 289 0

Fax +49 30 533 289 900

Niederlassung

Nürnberg

Zeltnerstraße 3
90443 Nürnberg

Fon +49 911 8819 7263

Fax +49 30 533 289 900