HISOLUTIONS

BERICHT ZUR IS-KURZREVISION

Final

Stand 26. Oktober 2021

DATAPORT

- VERTRAULICH -

RECHTLICHE HINWEISE

DOKUMENTEN-STATUS

Projektname	Projektnummer
21.Dataport.iKfz Audit und Pentest	57070

Dokumenten-Titel

Bericht zur IS-Kurzrevision

Autor	Seiten	Version	Verfasst am
[redacted] [redacted]@hisolutions.com	18	Final v1	26. Oktober 2021

VERSIONSVERLAUF

Datum	Version	Beschreibung	Bearbeiter
27.07.2021	0.1	Dokumentenstruktur	[redacted]
27.08.2021	0.2-0.4	Entwurf	[redacted]
31.08.2021	0.5	QS	[redacted]
26.10.2021	1.0	Finalisierung	[redacted]

MANAGEMENT SUMMARY

1.1 Rahmendaten

Revisionsgegenstand	**i-Kfz-relevante Prozesse und Systeme, teilweise Informationsverbund (Gesamt)**
Revisionsteam	[redacted]
Ansprechpartner	[redacted]
Anlass	Antrag auf Zulassung des iKFZ-Angebots beim KBA
Grundlagen und Anforderungen	BSI Leitfaden IS-Revision (Version 3.0, März 2018) Verbindliche Prüfthemen für die IS-Kurzrevision (Version 2.0 vom 24.5.2018)
Zeitlicher Ablauf	Prüfung vor Ort: 29./30. Juli 2021 Übergabe Revisions-Bericht: 27.10.2021
Verteiler	[redacted]

1.2 Festgestellte Mängel

Es wurden insgesamt 21 Feststellungen ausgesprochen. Die nachfolgende Tabelle zeigt eine Schnellreferenz über die festgestellten Mängel. Eine detaillierte Übersicht findet sich in Kapitel 4.

	schwerwiegende Sicherheitsmängel	festgestellte Sicherheitsmängel	Sicherheitsempfehlungen
ISMS, ORP, CON, OPS, DER: Übergreifende Aspekte	**E1.1, E1.2, E1.3, E1.4, E1.5**	**E1.7, E1.7, E1.8, E1.9**	**E1.10, E1.11, E1.12, E1.13**
INF: Infrastruktur	-	**E2.1, E2.2**	-

HISOLUTIONS

	schwerwiegende Sicherheitsmängel	festgestellte Sicherheitsmängel	Sicherheitsempfehlungen
SYS: IT-Systeme	E3.1	E3.2	E3.3
Schicht 4 - NET: Netze	-	-	-
APP: IT-Anwendungen	-	E5.1, E5.2	E5.3

INHALTSVERZEICHNIS

2 ÜBERBLICK ÜBER DIE DURCHFÜHRUNG

2.1 Vorgehen IS-Kurzrevision

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

Bei der IS-Kurzrevision geht das IS-Revisionsteam nicht maßnahmen-, sondern themenorientiert vor. Die Prüfthemen sind in der Ergebnisübersicht in Kapitel 4 dargestellt.

2.2 Anmerkungen zur Durchführung

Das Revisionsteam wurde zu jeder Zeit freundlich und konstruktiv unterstützt. Es standen für alle Prüfthemen kompetente und aufgeschlossene Ansprechpartner zur Verfügung.

Der Zutritt zu den Räumlichkeiten und der Zugang zu den Systemen war zu jeder Zeit sichergestellt, und auch auf kurzfristige Anfragen der Revisoren wurde flexibel reagiert.

In Abstimmung mit dem KBA wurde der Betrachtungsgegenstand in der IS-Kurzrevision beschränkt auf alle Themengebiete, die nicht bereits durch vorhandene Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz abgedeckt sind. Diese Zertifizierungen umfassen das ISMS bei Dataport, den Systembetrieb im Twin-Datacenter sowie die vorhandenen Netzinfrastrukturen. In der IS-Kurzrevision erfolgte daher eine Prüfung der Fachanwendungen iKFZ und VIATO-Z einschließlich der dafür erstellten IT-Sicherheitskonzepte, die zur Administration eingesetzten Client-PCs sowie der VPN-Kopfstelle am Standort Altenholz, über die die Kommunikation zum KBA realisiert ist.

HISOLUTIONS

3 ERGEBNISÜBERSICHT

Die Ergebnisse der IS-Kurzrevision sind in den nachfolgenden Tabellen in Übersichtsform dargestellt und geben den Gesamtstatus der IT-Sicherheit zum Prüfgegenstand wieder. Die festgestellten Sicherheitsmängel sind nachfolgend in Kapitel 4 detailliert beschrieben.

3.1 Themenfeld 1 – Schichten ISMS, ORP, CON, OPS, DER

Prüfthema	Prüfergebnis	
Sicherheitsorganisation	abgedeckt durch den Zertifizierungsverbund TwinDC	
Sicherheitsmanagement	abgedeckt durch den Zertifizierungsverbund TwinDC	
Sicherheitsleitlinie	abgedeckt durch den Zertifizierungsverbund TwinDC	
kritische Geschäftsprozesse	abgedeckt durch den Zertifizierungsverbund TwinDC	
Sicherheitskonzept	Schwere Sicherheitsmängel	E.1.1, E.1.2, E.1.3, E.1.5, E.1.6, E.1.10, E.1.11
Personal	abgedeckt durch den Zertifizierungsverbund TwinDC	
Versions- und Änderungsmanagement	abgedeckt durch den Zertifizierungsverbund TwinDC	
Schulung und Sensibilisierung	abgedeckt durch den Zertifizierungsverbund TwinDC	
Behandlung von Sicherheitsvorfällen	abgedeckt durch den Zertifizierungsverbund TwinDC	
Notfallkonzept	Sicherheitsmängel	E.1.7, E.1.8, E.1.12
Datensicherung	abgedeckt durch den Zertifizierungsverbund TwinDC	
Outsourcing	Schwere Sicherheitsmängel	E.1.4, E.1.9, E.1.13

3.2 Themenfeld 2 – Schicht INF

Eine Betrachtung erfolgte für den RZ-Standort in Altenholz mit der VPN-Kopfstelle. Die übrigen Systeme werden im Twin-DC betrieben. Die Standorte dazu sind im Zertifizierungsverbund Twin-DC enthalten.

Prüfthema	Prüfergebnis	
Elektrische Verkabelung, IT-Verkabelung, Versorgungsleitungen	Keine Mängel festgestellt	
Zutrittskontrolle	Keine Mängel festgestellt	
Brandschutz	Sicherheitsmängel	E.2.1, E.2.2
Klimatisierung	Keine Mängel festgestellt	
Stromversorgung	Keine Mängel festgestellt	

3.3 Themenfeld 3 – Schicht SYS

Prüfthema	Prüfergebnis	
Sichere Grundkonfiguration der Server und Clients	Schwere Sicherheitsmängel	E.3.1, E.3.3
Berechtigungsvergabe	Sicherheitsmängel	E.3.2
mobile Endgeräte	Mobile Endgeräte kommen im Zusammenhang mit i-KFZ nicht zum Einsatz	
Multifunktionsgeräte	Multifunktionsgeräte kommen im Zusammenhang mit i-KFZ nicht zum Einsatz	
Mobile Datenträger und Datenträgeraustausch	abgedeckt durch den Zertifizierungsverbund TwinDC	

3.4 Themenfeld 4 – Schicht NET

Prüfthema	Prüfergebnis	
Netzdokumentation und Netzverwaltung	abgedeckt durch die Zertifizierungsverbünde TwinDC und Zugangsnetz	
Netzwerk- und System-management	abgedeckt durch die Zertifizierungsverbünde TwinDC und Zugangsnetz	
Konfiguration und sicherer Betrieb der Netzkompo-nenten	abgedeckt durch die Zertifizierungsverbünde TwinDC und Zugangsnetz	
Sicherung der Netzwerkzugänge	abgedeckt durch die Zertifizierungsverbünde TwinDC und Zugangsnetz	
Sicherheitsgateways	abgedeckt durch die Zertifizierungsverbünde TwinDC und Zugangsnetz	

3.5 Themenfeld 5 – Schicht APP

Prüfthema	Prüfergebnis	
E-Mail/Webauftritt	Der Einsatz von E-Mail ist über den Zertifizierungsverbund TwinDC abgedeckt. Die Anwendungen sind in die Web-Landesportale von Schleswig-Holstein und Hamburg eingebunden und verfügen nicht über einen eigenen Webauftritt.	
Anwendungen	Sicherheitsmängel	E.5.1, E.5.2, E.5.3

4 FESTGESTELLTE SICHERHEITSMÄNGEL

Soweit nicht näher bezeichnet, gelten die aufgeführten Feststellungen für alle vergleichbaren Zielobjekte des Informationsverbundes. Schwerwiegende Sicherheitsmängel sind gesondert gekennzeichnet.

4.1 Themenfeld 1 – Schichten ISMS, ORP, CON, OPS, DER

Schwerwiegender Sicherheitsmangel	**E.1.1 Keine Schutzbedarfsfeststellung nach BSI-Standard**
Beschreibung:	In den IT-Sicherheitskonzepten für die Anwendungen VIATO-Z und iKFZ fehlt die Herleitung des Schutzbedarfs. Der Schutzbedarf wurde in Form eines Formblatts mit Ergebnissen für die Anwendung vorgegeben. Eine Schutzbedarfsfeststellung nach BSI-Standard mit Begründung und Bezug zu den Grundwerten und Schadensszenarien ist nur im Sicherheitskonzept für iKFZ enthalten, bei VIATO-Z fehlt sie. Die ermittelten Schutzbedarfe sind daher nicht nachvollziehbar. Eine Ableitung des Schutzbedarfs von der Anwendung auf die einzelnen Zielobjekte unter Berücksichtigung von Maximalprinzip, Verteilungs- und Kumulationseffekt ist in beiden Sicherheitskonzepten nicht erfolgt. Gemäß den vertraglichen Vereinbarungen zwischen Dataport und seinen Auftraggebern ist die Schutzbedarfsfeststellung eine Beistellung des Auftraggebers.
Empfehlung:	Fordern Sie vom Auftraggeber eine vollständige Schutzbedarfsfeststellung nach BSI-Standard ein und nehmen Sie diese in die Sicherheitskonzepte auf.

Schwerwiegender Sicherheitsmangel	**E.1.2 Kein nachvollziehbare Risikoanalyse im Sicherheitskonzept für VIATO-Z**
Beschreibung:	Die Risikobewertung im Sicherheitskonzept für die Anwendung VIATO-Z fehlt. Damit ist nicht nachvollziehbar, wie die vorgeschlagenen Zusatzmaßnahmen aus den betrachteten Risiken abgeleitet werden. Weiter ist nicht prüfbar, ob die Risikobetrachtung vollständig und angemessen erfolgt ist. Gemäß den vertraglichen Vereinbarungen zwischen Dataport und seinen Auftraggebern ist die Risikoanalyse eine Beistellung des Auftraggebers.
Empfehlung:	Fordern Sie vom Auftraggeber eine vollständige Risikoanalyse nach BSI-Standard ein und nehmen Sie diese in die Sicherheitskonzepte auf.

Schwerwiegender Sicherheitsmangel	**E.1.3 Unvollständiger IT-Grundschutzcheck**

Beschreibung:	Im IT-Grundschutzcheck in den Sicherheitskonzepten für VIATO-Z und iKFZ werden zahlreiche Anforderungen als „entbehrlich“ markiert, weil sie in der Umsetzungsverantwortung des Auftraggebers liegen. Das ist aus Sicht von Dataport korrekt und spiegelt auch die vertraglichen Vereinbarungen mit den Auftraggebern wider. Allerdings sind die Sicherheitskonzepte dadurch unvollständig und nicht geeignet, die Umsetzung eines geeigneten Sicherheitsniveaus nachzuweisen, ohne dass ein ergänzender Nachweis der Umsetzung der Anforderungen in der Verantwortung des Auftraggebers geführt wird.
Empfehlung:	Fordern Sie von Ihrem Auftraggeber die einen IT-Grundschutzcheck über alle ihm zugeordneten Anforderungen ein und fügen Sie diesen als Anlage den Sicherheitskonzepten bei. Stimmen Sie mit dem Auftraggeber ein Verfahren für die übergreifende Realisierungsplanung aller defizitären Maßnahmen ab.

Schwerwiegender Sicherheitsmangel	**E.1.4 Fehlende Mitwirkungsleistungen des Auftraggebers**
Beschreibung:	In der Leistungsbeschreibung des Betriebsvertrags existiert ein Security Service-Level-Agreement (SSLA), das umfangreiche Themen in die Verantwortung des Auftraggebers einordnet bzw. auslagert. Hierzu gehören unter anderem die Schutzbedarfsfeststellung, die Risikoanalyse sowie die auftraggeberseitige Umsetzung von Grundschutz-Anforderungen. Diese werden damit außerhalb des Verantwortungsbereichs von Dataport eingeordnet. Die Ergebnisse der seitens Auftraggeber zugeordneten Bestandteile liegen in den geprüften IT-Sicherheitskonzepten zu VIATO-Z und iKFZ größtenteils nicht vor. Die vertragliche vereinbarte Aufteilung der Zuständigkeiten im IT-Sicherheitsmanagement scheint in der Praxis nicht zu funktionieren.
Empfehlung:	Klären Sie den Sachverhalt mit dem Auftraggeber und vereinbaren und dokumentieren Sie eine praktikable Regelung zur Erstellung und Fortschreibung vollständiger Sicherheitskonzepte für die Anwendungen.

Schwerwiegender Sicherheitsmangel	**E.1.5 Fehlende Betrachtung der VPN-Kopfstelle in den Sicherheitskonzepten**
Beschreibung:	Die VPN-Kopfstelle am Standort Altenholz ist nicht in den Zertifizierungsverbünden von Dataport enthalten. Sie wird aber auch in den anwendungsspezifischen Sicherheitskonzepten nicht betrachtet, ohne dass der Ausschluss dort begründet ist oder ein Verweis auf eventuelle weitere vorhandene Sicherheitskonzepte besteht. Ein Nachweis der Sicherheit der VPN-Kopfstelle ist in den übergebenen Dokumenten nicht geführt.

Empfehlung:	Nehmen Sie die Betrachtung der VPN-Kopfstelle an geeigneter Stelle in mindestens eines der anwendungsbezogenen IT-Sicherheitskonzepte auf, oder verweisen Sie auf eine ggf. vorhandene separate Sicherheitsbetrachtung dafür.

Sicherheitsmangel	**E.1.6 Unfertiges IT-Sicherheitskonzept für iKFZ**
Beschreibung:	Das anwendungsbezogene IT-Sicherheitskonzept für iKFZ liegt nur in einer Entwurfsversion 0.0.1 vor und ist bisher nicht freigegeben. Ein Realisierungsplan über die defizitären Grundschutzmaßnahmen ist im vorgelegten Entwurf noch nicht enthalten.
Empfehlung:	Vervollständigen Sie das IT-Sicherheitskonzept für iKFZ und geben Sie dieses frei.

Sicherheitsmangel	**E.1.7 Unvollständiges „Notfallhandbuch RZ²“**
Beschreibung:	Das „Notfallhandbuch RZ²“ enthält für viele Schadensszenarien keine Anleitungen zur Bewältigung, sondern legt jeweils nur Meldewege fest. An einigen Stellen werden reaktive Maßnahmen jedoch unter der Überschrift „Vorbeugende Maßnahmen“ aufgeführt. Dies wirkt insgesamt unsystematisch und stellt insbesondere nicht sicher, dass beim Eintreten des jeweiligen Notfalls tatsächlich geeignete Bewältigungsmaßnahmen ergriffen werden.
Empfehlung:	Überarbeiten Sie das Notfallhandbuch systematisch und legen Sie für jedes betrachtete Notfallszenario konkrete Notfallbehandlungsmaßnahmen fest.

Sicherheitsmangel	**E.1.8 Keine auffindbaren Wiederanlaufpläne**
Beschreibung:	Die Wiederanlaufpläne, die im Notfallhandbuch RZ² referenziert werden, waren im Rahmen der Revision nicht aufzufinden. Notfallpläne müssen so hinterlegt sein, dass beim Eintreten der Notfallsituation ein schneller Zugriff erfolgen kann.
Empfehlung:	Hinterlegen Sie die Wiederanlaufpläne an einer gut auffindbaren Stelle und machen Sie diese bei Ihren Mitarbeitern bekannt.

Sicherheitsmangel	**E.1.9 Veraltetes Security Service-Level-Agreement**

Beschreibung:	Die Inhalte des Security Service-Level-Agreement (SSLA) beziehen sich noch auf die Grundschutz-Standards 100-X des BSI. Aktuell gültig sind jedoch die BSI-Standards 200-X Bei der Erstellung der anwendungsbezogenen Sicherheitskonzepte wurden die neuen Standards auch bereits angewendet.
Empfehlung:	Aktualisieren Sie die SSLA.

Sicherheitsempfehlung	**E.1.10 Fehlende Erläuterung zur Modellierung im Sicherheitskonzept für Viato-Z**
Beschreibung:	In der Modellierung des Sicherheitskonzeptes für Viato-Z sind bestimmte Bausteine nicht enthalten, da sie komplett dem Dataport-Standard entsprechen, im Sicherheitskonzept des TwinDC betrachtet werden und Teil der Zertifizierungsverbünde sind. Hierzu gehören unter anderem die Bausteine OPS.1.1.5, APP.3.2, APP.4.3 sowie die gesamte Schicht SYS. Eine Erläuterung fehlt jedoch, wodurch das Modellierungsdokument nicht nachvollziehbar ist.
Empfehlung:	Begründen Sie in der Modellierung, welche Bausteine aus welchen Gründen nicht betrachtet werden.

Sicherheitsempfehlung	**E.1.11 Inkonsistente Aussage zur Risikoanalyse für VIATO-Z**
Beschreibung:	In Kapitel 1.6 im IT-Strukturanalysedokument zum Sicherheitskonzept für VIATO-Z wird behauptet, dass keine Risikoanalyse durchgeführt wurde. Ergebnisse der Risikoanalyse sind jedoch im Sicherheitskonzept enthalten.
Empfehlung:	Berechtigen Sie den entsprechenden Absatz.

Sicherheitsempfehlung	**E.1.12 Keine Redundanz für das VPN-Gateway zum KBA**
Beschreibung:	Das VPN-Gateway zum KBA ist nicht redundant ausgelegt. Auskunftsgemäß ist ein Ersatzgerät vorhanden und kann kurzzeitig (innerhalb von geschätzten 30 Minuten) in Betrieb genommen werden. Für die Verfügbarkeit der Anwendungen insgesamt ist ein hoher Schutzbedarf ausgewiesen. Ein Herunterbrechen des Schutzbedarfs auf die VPN-Komponente ist nicht erfolgt. Es kann daher nicht beurteilt werden, ob die vorhandene Cold-Standby-Lösung zur Erfüllung des Schutzbedarfs geeignet ist.
Empfehlung:	Definieren Sie den Schutzbedarf des Gerätes entsprechend der Ableitungsregeln und der erfüllten Funktion. Überprüfen Sie die tatsächlich benötigte Zeit für eine Inbetriebnahme des Ersatzgeräts und

	verifizieren Sie die Angemessenheit dieser Lösung anhand des ermittelten Schutzbedarfs.

Sicherheitsempfehlung	**E.1.13 Nur informeller Austausch zwischen Auftraggeber und Dataport**
Beschreibung:	Der Austausch zwischen Auftraggeber und Dataport zu Sicherheitsthemen wie z. B. zu Sicherheitsvorfällen, zu Auswirkungen aus Weiterentwicklungen des Grundschutz-Kompendiums usw. findet nicht formell statt. Dies bedeutet, dass Informationen nur mündlich und/oder unregelmäßig mit dem Auftraggeber ausgetauscht werden.
Empfehlung:	Etablieren Sie eine systematische, regelmäßige Abstimmung zwischen Dataport und dem Auftraggeber zum IT-Sicherheitsmanagement.

4.2 Themenfeld 2 – Schicht INF

Sicherheitsmangel	**E.2.1 Feuerlöscher außerhalb des Wartungsfensters**
Beschreibung:	Bei der letzten Feuerlöscherwartung wurde ein Gerät im Rechenzentrum am Standort Altenholz an einer Säule in der Raummitte des Betriebsraumes nicht geprüft. Die nächste Wartung sollte laut Aufkleber 07/19 stattfinden. Alle weiteren im Raum befindlichen Geräte hatten eine aktuelle Wartung.
Empfehlung:	Tauschen Sie den Feuerlöscher aus bzw. holen Sie die Wartung nach und prüfen Sie den aktuellen Wartungsprozess.

Sicherheitsmangel	**E.2.2 Lagerung unnötiger Gegenstände im Betriebsraum**
Beschreibung:	Im Serverschrank direkt neben dem Betriebsschrank mit den Geräten der VPN-Kopfstelle am Standort Altenholz lagert unnötiges Material (Kabel, Verpackungen), was die Brandlast im Raum unnötig erhöht.
Empfehlung:	Entfernen Sie unnötiges Material in der Nähe der Betriebsschränke und sehen Sie von einer Lagerung von insbesondere brennbarem Material auch „übergangsweise“ ab.

4.3 Themenfeld 3 – Schicht SYS

Schwerwiegender Sicherheitsmangel	**E.3.1 Einsatz von nicht mehr unterstützten Geräten in der VPN-Kopfstelle**

Beschreibung:	In der VPN-Kopfstelle kommen Cisco-Komponenten der Typen 2960-G und 892 zum Einsatz. Diese haben bereits ihr End-Of-Life (EOL) überschritten und erhalten keinen Support und keine Sicherheitsupdates vom Hersteller mehr. Die Geräte verwenden dabei eine Firmware der Version Cisco iOS 15.2. Die aktuelle Version ist Cisco iOS 15.9. In den eingesetzten Komponenten sind daher mit großer Wahrscheinlichkeit unbehandelte Sicherheitslücken vorhanden.
Empfehlung:	Wechseln Sie die Cisco-Komponenten durch aktuelle Systeme aus und prüfen Sie Ihren Wartungs- und Updateprozess.

Sicherheitsmangel	**E.3.2 Keine Zugriffsdokumentation für das Notfallpasswort für die VPN-Kopfstelle**
Beschreibung:	Das Notfallpasswort für die Geräte der KBA-VPN-Kopfstelle ist als Gruppenpasswort angelegt. Es erfolgt keine Zugriffsdokumentation. Geteilte Passwörter haben mehrere Probleme. So können zum Beispiel Änderungen nicht mehr einem Nutzer zugeordnet werden. Im Falle von maliziösen Verhalten ist zudem unter Umständen nicht klar, auf welche Weise das Passwort missbraucht wurde, ob also zum Beispiel ein interner oder externer Akteur gehandelt hat und damit auch ggf. auch auf welche Weise das Passwort „nach außen“ gedrungen ist.
Empfehlung:	Hinterlegen Sie Notfallpasswörter an sicherer Stelle (z. B. in verschlossenen Umschlägen in einem Safe) und dokumentieren Sie die Herausgabe und den Einsatz. Ändern Sie das Notfallpasswort nach der Nutzung und hinterlegen Sie das neue Passwort wieder sicher.

Sicherheitsempfehlung	**E.3.3 Kein Einsatz von Microsoft LAPS zur Verwaltung der lokalen Administratorkonten auf den Clients**
Beschreibung:	Bei der manuellen Prüfung ist aufgefallen, dass die verwendeten Clients aktuell über keine lokale Administratorenkontenverwaltung verfügen. Eine Lösung wie die Local Admin Password Solution(LAPS) von Microsoft wird also nicht eingesetzt. Die manuelle Verwaltung der lokalen Administratorkonten ist aufwändig und erleichtert ggf. Angriffe auf die Domäne, wenn Passwörter erraten oder mitgelesen werden können.
Empfehlung:	Führen Sie die Local Admin Password Solution (LAPS) von Microsoft oder eine alternative Lösung ein.

4.4 Themenfeld 4 – Schicht NET

Zu diesem Themenfeld wurden keine Prüfungen durchgeführt.

4.5 Themenfeld 5 – Schicht APP

Sicherheitsmangel	E.5.1 Fehlendes Mandantenkonzept
Beschreibung:	Im Sicherheitskonzept der Viato-Z liegen laut Kapitel 2.1 drei Mandanten vor. Im Kapitel 7 wird jedoch auf ein Mandantenkonzept verzichtet mit der Begründung, dass es nur einen Mandanten gebe. Dies stellt eine Inkonsistenz dar. Auf Grund der Erläuterung in Kapitel 2.1 ist dabei davon auszugehen, dass ein Mandantenkonzept benötigt wird.
Empfehlung:	Erstellen Sie ein Mandantenkonzept gemäß Anforderung.

Sicherheitsmangel	E.5.2 Kein Löschkonzept für die Protokollierung in i-KFZ
Beschreibung:	Die Anwendung i-KFZ nimmt eine umfassende Anwendungsprotokollierung in der Datenbank vor. Bisher ist dafür kein Löschkonzept definiert und umgesetzt, d. h. die Protokolleinträge verbleiben auf unbestimmte Zeit in der Datenbank. Die unbefristete Speicherung von Protokolldaten stellt eine Datenschutzverletzung dar. Durch den fortlaufenden Verbrauch von Speicherplatz können sich ggf. Probleme beim Erreichen der vorhandenen Speicherkapazität ergeben.
Empfehlung:	Prüfen Sie die Einführung eines Löschkonzepts für die Protokollierung der Datenbank im i-KFZ.

Sicherheitsempfehlung	E.5.3 Deaktivierungsoption für TLS im VIATO-Z-Client.
Beschreibung:	Die Oberfläche der Anmeldemaske im Client für Viato-Z verfügt über eine Checkbox „TLS“, über die vermutlich eine Deaktivierung von TLS von Clientseite erfolgt. Im Test wurde ein entsprechender Verbindungsversuch jedoch serverseitig abgelehnt.
Empfehlung:	Es sollte mit dem Hersteller Viato-Z geprüft werden, ob die Checkbox im Client zum Deaktivieren der TLS-Verbindung erforderlich ist. Eine Deaktivierung von TLS ergibt nur zu Zweckend es Debugging oder bei der Nutzung einer Proxy-Konfiguration Sinn und sollte in diesem Fall eher durch eine Firewall durch SSL Intercept abgebildet werden, da hier in der Regel kontrolliert geprüft werden kann.

HISOLUTIONS

ANHANG A LISTE DER SICHERHEITSMÄNGEL

KONTAKT

[redacted]

Fon +49 30 533289-0

[redacted]@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	Niederlassung	Niederlassung
Frankfurt am Main	**Bonn**	**Nürnberg**
Mainzer Landstraße 50	Heinrich-Brüning-Str. 9	Zeltnerstraße 3
60325 Frankfurt am Main	53113 Bonn	90443 Nürnberg
Fon +49 30 533 289 0	Fon +49 228 52 268 175	Fon +49 911 8819 7263
Fax +49 30 533 289 900	Fax +49 30 533 289 900	Fax +49 30 533 289 900