Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verordnung über die Arbeits- und Ruhezeit der berufsmässigen Führer von leichten Personentransportfahrzeugen und schweren Personenwagen (ARV 2)

Änderung vom …

Der Schweizerische Bundesrat
verordnet:

I

Die Verordnung vom 6. Mai 1981[1] über die Arbeits- und Ruhezeit der berufsmässigen Führer von leichten Personentransportfahrzeugen und schweren Personenwagen wird wie folgt geändert:

Ingress

gestützt auf die Artikel 25 Abs. 2[bis], 56, 103 und 106 des Strassenverkehrsgesetzes vom 19. Dezember 1958[2],

Art. 14 Bst. a[bis]

Zur Kontrolle der Einhaltung der Arbeits-, Lenk- und Ruhezeit (Art. 5–12) dienen namentlich:

a[bis]. die Eintragungen in der elektronischen Applikation (Art. 16*b*–16*g*);

Art. 16b Elektronische Applikation

Die elektronische Applikation dient der Erfassung der Verarbeitung, der Anzeige und der Übermittlung von Informationen zu den Arbeits-, Lenk- und Ruhezeiten von berufsmässigen Führern (Daten) mittels eines Softwareprogramms, das auf einem Datenendgerät installiert oder über ein Datennetz genutzt wird.

SR .....
1 SR **822.222**
2 SR **741.01**

Art. 16c Anforderungen an die elektronische Applikation

[1] Die elektronische Applikation muss folgende Anforderungen erfüllen:

a. Es müssen die Daten nach den Artikeln 16*g* sowie 18 Absätze 5 und 6 erfasst und elektronisch freigegeben werden können.

b. Der Zeitpunkt der Erfassung der Daten muss ersichtlich sein.

c. Jede Veränderung erfasster Daten muss ersichtlich sein und auf eine einfache Art nachvollzogen und überprüft werden können.

d. Die Daten müssen nach jeder Eingabe automatisch und verzögerungsfrei erfasst und gespeichert werden.

e. Die erfassten Daten müssen sofort ersichtlich und während mindestens 28 Tagen uneingeschränkt und vollständig abrufbar sein; nach Ablauf dieses Zeitraums dürfen die Daten gelöscht oder überschrieben werden.

f. Die erfassten Daten müssen für die Kontrollbehörden zugänglich sein:

1. in der in Anhang 1 dargestellten Form mit der Möglichkeit für die Kontrollbehörden, die Daten vor Ort mit standardisierten Mitteln zu sichern,

2. online über eine eindeutige URL, beispielsweise in Form eines QR-Codes.

g. Die Daten und ihre Übertragung müssen vor Manipulation und vor unbefugtem Zugriff geschützt sein.

h. Die elektronische Applikation muss mit einer fortlaufenden Nummer zur eindeutigen Identifikation der beim jeweiligen Führer installierten Kopie und der Identifikation des Zertifikats versehen sein.

[2] Die elektronische Applikation kann zusätzliche Funktionen aufweisen, die mit der Fahrt in Zusammenhang stehen, sofern dadurch die Erfüllung der Anforderungen nach Absatz 1 nicht beeinträchtigt wird.

Art. 16d Zertifizierung der elektronischen Applikation

[1] Die elektronische Applikation ist einer Zertifizierungsstelle nach Artikel 16*e* zur Prüfung und Zertifizierung vorzulegen. Die Prüfung erfolgt nach einem Zertifizierungsschema auf der Basis der Richtlinien nach Anhang 2 Ziffer 2. Erfüllt die Applikation die Anforderungen nach Artikel 16*c*, so erhält der Inhaber der Applikation ein Zertifikat (Zertifikatsinhaber). Das Zertifikat wird für eine Dauer von maximal fünf Jahren ausgestellt.

[2] Der Zertifikatsinhaber muss der Zertifizierungsstelle:

a. jede wesentliche Funktionsänderung an der Applikation zur Überprüfung und Freigabe vorlegen;

b. jährlich die Vorkommnisse, die auf mögliche Funktionsstörungen hinweisen, melden.

[3] Das Zertifikat kann auf Gesuch des Zertifikatsinhabers jeweils um maximal weitere fünf Jahre verlängert werden, sofern die Anforderungen nach Artikel 16*c* weiterhin

erfüllt sind. Die Zertifizierungsstelle führt dazu ein Audit durch. Das Gesuch um Verlängerung muss vor Ablauf der Gültigkeit des Zertifikats gestellt werden.

4 Bei vertragsrechtlichen Streitigkeiten zwischen der Zertifizierungsstelle und dem Gesuchsteller oder dem Zertifikatsinhaber entscheidet das Zivilgericht.

Art. 16e Anforderungen an die Zertifizierungsstelle

Die Zertifizierung der elektronischen Applikation darf ausschliesslich durch Stellen erfolgen, die:

a. nach der Norm ISO/IEC 17065:2013, Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren für die folgenden Bereiche akkreditiert sind:
   1. Kryptographie und sichere Kommunikation,
   2. Datenschutz,
   3. Sicherheit der mobilen Applikation; und
b. den Anforderungen in Anhang°2 entsprechen.

Art. 16f Bedingungen für die Verwendung der elektronischen Applikation

1 Die elektronische Applikation darf für Fahrzeuge verwendet werden, deren Fahrzeugausweis einen Eintrag nach Artikel 80 Absatz 2 der Verkehrszulassungsverordnung vom 27. Oktober 1976[3] (VZV) enthält und die nicht mit einem Fahrtschreiber ausgerüstet sind.

2 Der Führer eines Fahrzeugs muss dem ASTRA vor der Verwendung der elektronischen Applikation die Identifikationsnummer nach Artikel 16*c* Absatz 1 Buchstabe h mitteilen. Ein Führer darf maximal zwei Applikationen einsetzen.

3 Der Führer muss dafür sorgen, dass das Datenendgerät:

a. stets gemäss dem neuesten Stand vor Manipulation und unbefugtem Zugriff geschützt ist;
b. wirksam gegen jegliche mechanische Belastung geschützt und ständig mit ausreichend Energie versorgt ist.

4 Er unterstützt die Kontrollbehörden auf Verlangen beim Zugriff auf die Daten.

Art. 16g Erfassung der Arbeits-, Lenk- und Ruhezeiten in der elektronischen Applikation

1 Der Führer muss die Daten nach Artikel 18 Absätze 5 und 6 erfassen und allfällige automatische Einträge überprüfen. Er muss die Eintragungen laufend vornehmen. Die Eintragungen müssen nicht grafisch erfolgen.

2 Führt der berufsmässige Führer mit dem Fahrzeug eine Privatfahrt aus, so muss er diese vor Fahrtantritt in der elektronischen Applikation entsprechend kennzeichnen. Er muss Beginn, Ende und Fahrleistung der Privatfahrt erfassen.

3 SR **741.51**

[3] Führen Dritte mit dem Fahrzeug eine Privatfahrt aus, so muss der berufsmässige Führer vor Beginn seiner nächsten berufsmässigen Fahrt die dabei entstandene Kilometerdifferenz sowie den Vermerk «anderer Führer/andere Führerin» in der elektronischen Applikation erfassen.

[4] Der Führer muss dem Arbeitgeber die Daten der elektronischen Applikation zu den Arbeits-, Lenk- und Ruhezeiten spätestens am ersten Arbeitstag der folgenden Woche zur Verfügung stellen.

Art. 19 Abs. 7

[7] Auf die Führung des Arbeitsbuchs kann verzichtet werden, wenn die Arbeits-, Lenk- und Ruhezeiten mit einer elektronischen Applikation erfasst werden.

Art. 21 Abs. 1 Einleitungssatz und 2

[1] Der Arbeitgeber überwacht laufend anhand der verfügbaren Unterlagen, wie Einlageblätter und Wochenbündel des Fahrtschreibers, Eintragungen in der elektronischen Applikation, Wochen- und Tagesblätter der Arbeitsbücher, allfällige betriebsinterne Tagesrapporte und Kontrollkarten (Art. 19 Abs. 1, Art. 25 Abs. 4), ob die Bestimmungen über die Arbeits-, Lenk- und Ruhezeit (Art. 5–12) eingehalten worden sind. Er hält dazu für jeden Führer folgende Angaben in einer Aufstellung fest:

[2] Für Arbeitnehmer, deren tägliche Lenkzeit aufgrund einer summarischen Überprüfung der Kontrollmittel nach Artikel 14 Buchstaben a und a^{bis} offensichtlich weniger als 7 Stunden betragen hat, ist in der Aufstellung kein Eintrag der Lenkzeit erforderlich; es genügt, diese bei der Ermittlung der täglichen Arbeitszeit (Abs. 1 Bst. b) einzubeziehen.

Art. 22 Abs. 3–5

[3] Er muss dem Führer das Arbeitsbuch sowie die für den Fahrtschreiber erforderlichen Schlüssel und Einlageblätter oder die elektronische Applikation zur Verfügung stellen. Der Führer muss dem Arbeitgeber einen allfälligen Defekt des Fahrtschreibers oder der elektronischen Applikation so rasch als möglich melden.

[4] Der Arbeitgeber muss ein Verzeichnis führen, in dem die Namen der Führer, ihre Adresse und ihr Geburtsjahr sowie die Nummern ihrer Arbeitsbücher eingetragen sind.

[5] Er muss dafür sorgen, dass Personendaten der Führer, die im Zusammenhang mit der Durchführung dieser Verordnung bei ihm anfallen, nur für die Zwecke dieser Verordnung verwendet und gegen unbefugten Zugriff geschützt werden.

Art. 23 Abs. 3 Einleitungssatz und Bst. b^{bis}

[3] Sie müssen am Geschäftssitz während zweier Jahre aufbewahren:

b^{bis}. die Eintragungen in der elektronischen Applikation (Art. 16*f* und 16g);

Art. 28 Abs. 2 Bst. d, e und f

2 Mit Busse wird bestraft, wer die Kontrollbestimmungen (Art. 15–23) verletzt, insbesondere wer:

d. die vorgeschriebenen Daten nicht oder nicht ordnungsgemäss auf der elektronischen Applikation erfasst;

e. das Gesamtsystem (elektronische Applikation, Datenendgerät und zentral gespeicherten Daten) so manipuliert, dass es falsche Daten liefert;

f. nicht zertifizierte elektronische Applikationen verwendet.

Art. 32 Abs. 1bis

1bis Es führt die Anhänge nach.

II

Diese Verordnung erhält neu die Anhänge 1 und 2 gemäss Beilage.

III

Diese Verordnung tritt am ... in Kraft.

… Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Karin Keller-Sutter
Der Bundeskanzler: Viktor Rossi

Anhang 1
(Art. 16*c* Abs. 1 Bst. e

Formblätter für die Erfassung der Arbeits-, Lenk- und Ruhezeiten

1. Allgemeines

Die Formblätter (1.1–1.4), welche die nach Artikel 18 Absätze 5 und 6 erforderlichen Angaben enthalten, sind verbindlich.

1.1 Tagesblatt für Arbeitnehmer

Feld	**Eintrag**
Name/Vorname	
Arbeitsbeginn	
Datum	
Kontrollschildnummer	
Kilometerstand (Beginn)	
Ruhezeit vor Dienstantritt in Std. und Min.	
Zeitlicher Verlauf/Tätigkeiten (Arbeitsbeginn und Arbeitsende) (Arbeitszeiten, Lenkzeiten, Pausen, Privatfahrten,)	

Arbeitsende	
Kilometerstand (Ende)	
Tageskilometer	
Kilometerdifferenz Privatfahrten	
Kilometerstand (inkl. Privatfahrten)	
Gesamtdauer je Tätigkeit	Lenkzeit
	Arbeitszeit:
	Pause:
Bemerkungen	
Unterschrift	

(Anhang 1.2)

1.2 Wochenblatt für Arbeitnehmer

Name/Vorname								
Woche								
Letzter wöchentlicher Ruhetag								
Wochentag	**MO**	**DI**	**MI**	**DO**	**FR**	**SA**	**SO**	**Wochentotal**
Kontrollschild								
Ruhezeit vor Beginn in Std. und Min.								
Arbeitsbeginn								
Arbeitsende								
Lenkzeit in Std. und Min.	.							
Arbeitszeit in Std. und Min.		.						
Pausen in Std. und Min.								
Summe Arbeits- und Lenkzeit in Std. und Min.								
Wöchentlicher Ruhetag								
Wöchentlicher freier Halbtag								
Bemerkungen								

(Anhang 1.3)

1.3 Tagesblatt für selbständigerwerbende Führer

Feld	Eintrag
Name/Vorname	
Datum	
Kontrollschildnummer	
Kilometerstand (Beginn)	
Ruhezeit vor Dienstantritt in Std. und Min.	
Zeitlicher Verlauf/Tätigkeiten (Beginn und Ende der Lenkzeit)	
Kilometerstand (Ende)	
Tageskilometer	
Gesamtdauer Lenkzeit in Std. und Min.	
Bemerkungen	
Unterschrift	

(Anhang 1.4)

1.4 Wochenblatt für selbständigerwerbende Führer

Name/Vorname								
Woche								
Letzter wöchentlicher Ruhetag								
Wochentag	**MO**	**DI**	**MI**	**DO**	**FR**	**SA**	**SO**	**Wochentotal**
Kontrollschild								
Ruhezeit vor Beginn in Std. und Min.								
Beginn der beruflichen Tätigkeit								
Ende der beruflichen Tätigkeit								
Lenkzeit in Std. und Min.								
Wöchentlicher Ruhetag								
Wöchentlicher freier Halbtag								
Bemerkungen								

Anhang 2
(Art. 16*d* Abs. 1 und 16*e*)

Anforderungen an Zertifizierungsstellen

1. Allgemeines

1.1 Zertifizierungsstelle

Jede Zertifizierungsstelle ist verpflichtet:

- unparteilich zu arbeiten und Interessenkonflikte zu vermeiden;
- die Vertraulichkeit von proprietären Informationen, des Quellcodes und der Sicherheitsdokumentation sicherzustellen;
- das Zertifizierungsschema konsistent anzuwenden;
- Aufzeichnungen über Bewertungen und Entscheidungen zu führen.

1.2 Zertifizierungsschema

Die Zertifizierungsstelle erstellt für das Prüfen der Konformität von elektronischen Applikationen mit den Anforderungen nach Artikel 16*c* Absätze 1 und 2 ein Zertifizierungsschema unter Berücksichtigung der Richtlinien nach Ziffer 2.

Sie stellt dabei die Übereinstimmung mit den Anforderungen dieser Verordnung und mit den relevanten internationalen Standards sicher (z. B. den Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie Norm SN EN ISO/IEC 15408:2023 Information security, cybersecurity and privacy protection Evaluation criteria for IT security (*Common Criteria*), den Normen SN EN ISO/IEC 62443-4-1:2018 und 62443-4-2:2019 IT-Sicherheit für industrielle Automatisierungssysteme, SN EN ISO/IEC 27034:2023 Information technology – Security techniques – Application security und NF EN ETSI 303645:2024 CYBER – Cybersécurité pour l'Internet des objets grand public: Exigences de base [4] sowie dem *Mobile Application Security Verification Standards* (MASVS) des *Open Worldwide Application Security Project* (OWASP)[5].

Sie verwaltet und aktualisiert das Zertifizierungsschema bei Bedarf.

4 Die Normen können kostenlos eingesehen und gegen Bezahlung bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch (zum Teil nur auf Englisch oder Französisch verfügbar).

5 Abrufbar unter: https://mas.owasp.org > MASVS (Version 2.1.0).

2. Richtlinien für das Zertifizierungsschema

2.1 Geltungsbereich und Grundsätze der Richtlinien

Das Zertifizierungsschema gilt für mobile Anwendungen und ihre verbundenen Dienste, die für die Prüfung der Anforderungen dieser Verordnung verwendet werden.

Die technischen Anforderungen werden aus den Zielen und den Anforderungen der *Common Criteria,* den Anforderungen dieser Verordnung und dem MASVS (OWASP) abgeleitet.

2.2 Planung der Aktivitäten

Die verschiedenen Phasen müssen von der Zertifizierungsstelle mit dem Antragsteller geplant und vereinbart werden.

2.3 Prüfung der relevanten Sicherheitsartefakte

Alle von der Anwendung implementierten Sicherheitsartefakte (z. B. Verfahren, Vorlagen, Werkzeuge und Testberichte, die während der Entwicklung der Applikation verwendet werden) müssen einer Desktop-Prüfung unterzogen werden.

Tabelle 1 «Sicherheitsanforderungen» listet die wichtigsten zu prüfenden Sicherheitsartefakte auf, basierend auf aktuellen Vorgaben und Standards für mobile Anwendungen. Es werden vier verschiedene Bewertungsstufen definiert.

Abkürzung	Beschreibung
BE	Basisprüfung. Das Element wird durch einfaches Lesen geprüft. Ziel ist es, den Text grundlegend zu erfassen und zu verstehen. Fragen, die sich der Prüfer stellen sollte: Was sagt der Text aus? Welche Informationen kann ich dem Text entnehmen?
CE	Kritische Prüfung. Das Element wird durch kritisches Lesen geprüft. Ziel ist es, zu beurteilen, wie der Text funktioniert, ihn zu analysieren, zu interpretieren und zu bewerten. Fragen, die sich der Prüfer stellen sollte: Wie funktioniert der Text? Wie wird argumentiert? Welche Annahmen liegen dem Text zugrunde? Was bedeutet der Text?
SE	Stichprobenprüfung. Das Element besteht aus mehreren Dokumenten oder Abschnitten, und ein systematisches Stichprobenverfahren wird angewendet, um einige davon zu prüfen. Die Prüftiefe für die ausgewählten Elemente entspricht der kritischen Prüfung. Die Auswahlkriterien basieren auf folgenden Prinzipien: Dokumente mit grösserer sicherheitsrelevanter Auswirkung werden priorisiert.
NE	Nicht geprüft. Das Element wird nicht geprüft.

Tabelle 1: Sicherheitsanforderungen

Tabelle 2 «Sicherheitsziele» legt die verbindlichen Sicherheitsziele und -kontrollen nach dem MASVS (OWASP) und den *Common Criteria* für mobile Anwendungen fest. Sie bilden die Grundlage für die Audits und müssen umfassend geprüft werden.

Bereich	Hauptanforderung	PP[6]	MASVS (OWASP)
Kryptographie	Verschlüsselung, Schlüsselmanagement, sichere Protokolle	FCS[7]	CRYPTO
Datenschutz	Verschlüsselung ruhender Daten, Zugriffskontrolle, Kommunikation	FDP[8]	STORAGE, NETWORK
Konfiguration & Management	Sichere Konfiguration, Verwaltung kritischer Funktionen	FMT[9]	PLATFORM, ARCH
Anti-Exploitation	Schutz vor Manipulationen, Integritätskontrollen, Codeverschleierung, Updates	FPT[10]	RESILIENCE, ARCH
Vertrauenswürdige Kanäle	Schutz von Daten während der Übertragung	FTP[11]	NETWORK
Datenschutz	Einwilligung des Nutzers zur Übertragung von PII	FPR[12]	PRIVACY
Root/Jailbreak-Erkennung	App erkennt kompromittierte Umgebung	n/a[13]	RESILIENCE-1, -2

Tabelle 2: Sicherheitsziele

Für spezifische Überprüfungs- und Testanforderungen können die *Common Criteria* oder des MASVS (OWASP) als Grundlage verwendet werden.

2.4 Prüfung unterstützender Prozesse – Stufe 1

Artefakte müssen reproduzierbar erstellt werden können. Dazu müssen unterstützende Prozesse im Managementsystem des Antragstellers definiert sein, und es muss eine Desktop-Prüfung der Prozesse durchgeführt werden, um deren Vollständigkeit und Korrektheit zu überprüfen.

Zu prüfendes Dokument	Erstüber-prüfung/ Überwachung wesentliche Änderung	Überwachung geringfügige Änderung
Handbuch für Cybersicherheitsmanagement	CE	BE
	BE wenn ISO27001	BE
Handbuch für Kontoverwaltung	CE	BE

6 *Protection Profile for Application Software* (Schutzprofil) der NIAP (*National Information Assurance Partnership*)
7 *Functional Class Cryptographic Support* (Kryptographische Unterstützung)
8 *Functional Class User Data Protection* (Schutz der Benutzerdaten)
9 *Functional Class Security Management* - Sicherheitsmanagement
10 *Functional Class Protection of the TSF* (*TOE Security Functions*) (Schutz der Sicherheitsfunktionen des Prüfobjekts)
11 *Functional Class Trusted Path/Channels* (vertrauenswürdiger Pfad/Kanal)
12 *Functional Class Privacy* (Datenschutz / Privatsphäre)
13 *not applicable* (nicht anwendbar)

		BE
Architekturbericht	CE	BE
Sicherheitsaudit-Bericht	SE	BE
Handbuch für Konfigurationsmanagement	CE	BE
Handbuch für Ereignismanagement	SE	BE
Handbuch für Incident-Response-Prozesse	SE	BE
Handbuch für Wartung & Patch-Management	SE	BE
Bericht zum Schutz vor Schadsoftware	SE	BE
Bericht zum Fernzugriff	CE	BE
Handbuch für sicheres Design	CE	BE
Handbuch für sichere Implementierung	CE	BE
Handbuch für Sicherheitstestprozesse	CE	BE
Handbuch für Sicherheitsupdates	CE	BE
SIS[14] Cybersicherheitsbericht	CE	BE
Analyse der drahtlosen Kommunikation	SE	BE

Tabelle 3: Prozessüberprüfung

2.5 Testen – Stufe 2

Die Zertifizierungsstelle kann drei verschiedene Ansätze wählen:

- Durchführung von eigenen Tests;
- Verwendung eines externen Testberichts;
- Testbeobachtungen.

Der letzte Ansatz kann mit dem zweiten kombiniert werden, wenn die Reputation des externen Testanbieters nicht sichergestellt werden kann.

2.5.1 - Testbeobachtungen

Fehlen klare Testanforderungen in den *vorhandenen* Standards, so muss der in diesem Schema definierte Testansatz, der technische Sicherheitsfunktionen abdeckt, verwendet werden. Tests, die in den Testeinrichtungen des Antragstellers durchgeführt werden, müssen gemäss dem unten beschriebenen Teststatus beobachtet werden. Für diese Tests können die Ergebnisse der Prüfung der relevanten Sicherheitsartefakte berücksichtigt werden.

Es sind folgende Tests möglich:

14 *Secure Internet Service* (Sicherer Internet Dienst)

a. *Performed by the customer and witness based on sampling* (P-Tests); sie werden vom Antragsteller durchgeführt; ein Teil der Tests wird stichprobenmässig von der Zertifizierungsstelle beobachtet;

b. *Performed and fully Witness* (PW); sie werden durch Beobachtung validiert.

Tests	Erstüberprüfung / Überwachung wesentliche Änderung	Überwachung geringfügige Änderung
Authentifizierungstests (Login, Sitzungen…)	PW	P
Autorisierungstests (Zugriffsrechte, unzuverlässige Elemente…)	PW	P
Logtests (Benachrichtigungen, Alarme, Protokollierung)	PW	PW
Kommunikationsrobustheitstests (Integrität, Protokollkonformität)	PW	PW
Schnittstellentests (Dateninjektion, Fuzzing, Eingabevalidierung)	PW	P
Verfügbarkeitstests (Stresstests)	PW	P
Penetrationstests	PW	P

Tabelle 4:Testbeobachtungsstrategie

2.5.2 Prüfung der Testspezifikationen und Testwerkzeuge

Vor jeder Testbeobachtung müssen dem leitenden Auditor der Testplan, die Spezifikation und spezifische Informationen zu den Testwerkzeugen und Testprozessen des Antragstellers vorgelegt werden. Bewertet werden:

a. Testabdeckung;

b. Testeffektivität;

c. Qualität der Testdokumentation;

d. Angemessenheit der Testwerkzeuge;

e. Validierungsnachweise der Testwerkzeuge;

f. Kompetenz des Personals;

g. Unternehmensprozesse.

2.5.3 Während der Testbeobachtung

Der leitende Auditor muss:

a. die Testsitzung beobachten, den Ablauf so wenig wie möglich stören und alle Fragen oder Klärungen vor Beginn der Tests stellen;

b. überprüfen, ob die Tests gemäss den vereinbarten Verfahren, dem Testplan und den Testspezifikationen durchgeführt werden;

c. überprüfen, ob die Tests von den im Plan benannten Testern durchgeführt werden;

c. die verwendeten Werkzeuge und deren Versionen notieren und mit den in der Spezifikation definierten abgleichen.

Der Leitende Auditor darf nicht:

a. aktiv an den Testaktivitäten teilnehmen oder eine Rolle oder eine Funktion übernehmen, die vom Personal des Antragstellers ausgeführt werden sollte;

b. Meinungen oder Vorschläge abgeben oder Fragen beantworten;

c. den Testprozess, die Einrichtung oder die Ergebnisse in irgendeiner Weise beeinflussen.

Der leitende Auditor kann den Test jederzeit unterbrechen, wenn eine schwerwiegende Nichtkonformität festgestellt wird, die die Testergebnisse ungültig machen würde. In diesem Fall wird dies dem Antragsteller unverzüglich mitgeteilt.

2.5.4 Ergebnisse der Testbeobachtung

Der leitende Auditor muss einen Bericht mit mindestens folgenden Angaben erstellen:

a. Datum, Uhrzeit, Ort;

b. beteiligtes Personal und ihre Rollen;

c. Ziel und Kontext der Tests;

d. Version der ausgeführten Testfälle;

e. Abweichungen zwischen erwarteten und tatsächlichen Ergebnissen;

f. Dritteinschätzung der Ergebnisse.

2.6 Auditierung – Stufe 3

Die Wirksamkeit und die Relevanz der Artefakte und der Prozesse müssen bewertet und die Einschätzung durch die relevanten Stakeholder muss bestätigt werden. Dazu wird nach der Vorprüfung der Sicherheitsartefakte und der zugehörigen Prozesse ein formelles Audit mit folgenden Schwerpunkten durchgeführt:

- Prüfung der Sicherheitsfunktionen des geprüften Objekts;
- Bewertung des Implementierungs- und Reifegrads der unterstützenden Prozesse.

Auditthemen sind insbesondere:

- Sicherheitsorganisation und Kompetenzen;
- kontinuierlicher Verbesserungsprozess;
- interne Cybersicherheits-Audits
- Lebenszyklus;
- Qualitätsmanagementsystem;

- Konfigurationsmanagement;
- Änderungsmanagement;
- Auswirkungsanalyse;
- Überprüfung und Verifikation;
- Dokumentationsstruktur und Vorlagen;
- Lieferantenmanagement;
- Nachentwicklungsprozesse (z. B. Produktüberwachung, Schwachstellenmanagement).

2.7 Prüfung – Zertifizierungsempfehlung

Basierend auf den Ergebnissen der Schritte 2.3–2.6 muss der leitende Auditor prüfen, ob alle Anforderungen für eine Zertifizierung erfüllt sind.

2.8 Entscheid über die Zertifizierung

Basierend auf der Prüfung durch den leitenden Auditor muss ein unabhängiges Gremium die Zertifizierungsempfehlung prüfen. Es entscheidet in der Folge über die Ausstellung des Zertifikats.

2.9 Bescheinigung, Lizenzierung

Die Zertifizierungsstelle erteilt dem Gesuchsteller das Recht, ein Zertifizierungszeichen zu verwenden. Dabei kann die Zertifizierungsstelle ein bereits bestehendes Zeichen weiterverwenden.

2.10. Überwachung

Die Cybersicherheits-Audits müssen sichergestellt sein. Dazu muss die zertifizierte Applikation für mobile Anwendungen kontinuierlich aktualisiert werden, und die Zertifizierungsstelle muss mindestens alle zwölf Monate ab der Zertifizierungsentscheidung Überwachungsaktivitäten durchführen. Die Überwachungsaktivitäten müssen mindestens umfassen:

- Vorfallüberwachung: Nachweis, dass der Antragsteller seine Anwendung überwacht und Vorfälle angemessen behandelt;
- Änderungsmanagement: Art der Durchführung von Updates und der Gewährleistung ihrer Sicherheit;
- Audit: Gespräche mit relevanten Stakeholdern zum Änderungsmanagement und zu einer kontinuierlichen Verbesserung.

Alle Änderungen am Produkt oder an unterstützenden Prozessen müssen systematisch nach ihrer Auswirkung auf die Sicherheitsziele und das Vertrauensniveau klassifiziert werden. Änderungen werden als geringfügig oder als wesentlich eingestuft:

- geringfügige Änderungen: Änderungen, welche die Kernfunktionalität, das Bedrohungsmodell oder die Konformität nicht beeinflussen (z. B. kosmeti-

sche Updates, Leistungsoptimierungen, Dokumentationsverbesserungen); sie erfordern meist nur Dokumentationsaktualisierungen oder eine begrenzte Prüfung;

- wesentliche Änderungen: Änderungen, welche die Sicherheitsfunktionen, die Architektur oder das Risikoprofil betreffen (z. B. neue Funktionen, signifikante Updates kryptographischer Mechanismen, Änderungen der Bedrohungslage); sie erfordern eine umfassendere Bewertung und gegebenenfalls eine (Teil-)Neuzertifizierung.

Die Zertifizierungsstelle ist für die Klassifizierung jeder Änderung und die Anwendung der angemessenen Bewertungstiefe verantwortlich.

2.11 Sistierung

Die Gültigkeit eines Zertifikats kann vorübergehend ausgesetzt werden, insbesondere wenn:

- die Überwachung eine Nichtkonformität zeigt, die keinen sofortigen Entzug erfordert;
- eine unsachgemässe Nutzung des Zertifikats oder des Zeichens nicht durch geeignete Massnahmen behoben wird;
- sonstige Verstösse gegen das Zertifizierungsschema oder die Verfahren der Zertifizierungsstelle vorliegen.

Die Sistierung wird dem Antragsteller schriftlich mitgeteilt. Die Anwendung kann während der Sistierung weiterhin registriert sein.

2.12 Rückzug

Ein Zertifikat wird zurückgezogen, wenn:

- die Überwachung eine schwerwiegende Nichtkonformität zeigt;
- ein Verstoss gegen die Vereinbarung zwischen dem Gesuchsteller und der Zertifizierungsstelle vorliegt;
- im Falle einer Sistierung keine angemessenen Massnahmen ergriffen werden;
- der Antragsteller das Zertifikat nicht verlängern möchte;
- Standards oder Regeln sich ändern und der Antragsteller die neuen Anforderungen nicht erfüllen kann oder will;
- das Produkt nicht mehr hergestellt wird oder der Antragsteller seine Tätigkeit aufgibt.

Der Rückzug wird schriftlich mitgeteilt. Der Zertifikatsinhaber muss alle Kunden innerhalb von maximal zehn Tagen nach der Benachrichtigung informieren und sie darauf hinweisen, dass die Applikation nicht mehr verwendet werden darf.

3. Änderung der Produktanforderungen

Werden die Anforderungen für die abgedeckten Produkte geändert, so muss die Zertifizierungsstelle den Antragsteller unverzüglich schriftlich über das Inkrafttreten und einen allfälligen Bedarf für eine ergänzende Prüfung informieren.