SRQ - Specification Related Question

SRQ-ID: 1163

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Software zur Datenzugriffskontrolle und Klassifikation von Daten
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 3.2, 3.2.1, 3.2.8

Stichwort: Software zur Datenzugriffskontrolle und Klassifikation von Daten

Frage:

Anforderung [A_03328] fordert, dass Systemzustände (Konfigurationsdaten und Softwarestände) für 10 Jahre wiederherstellbar aufgehoben werden müssen. Ist dieser lange Zeitraum für alle Bereiche der Telematikinfrastruktur verpflichtend?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Eine pauschale Anforderung an eine 10-jährige Wiederherstellbarkeit kann in einigen Bereichen der Telematikinfrastruktur zu Unverhältnismäßigkeiten führen. Grundsätzlich sind die Service-Level-Agreements (SLA) mit den Dienstbetreibern ausschlaggebend. Die pauschale Anforderung wurde daher auf 2 Jahre, mit einer täglichen Wiederherstellbarkeit für 30 Tage, reduziert, wobei für Software zur Datenzugriffskontrolle eine erweiterte Dokumentationspflicht durch den Dienstbetreiber in seinem Sicherheitskonzept gefordert wird. Dies schließt nun auch eine Klassifizierung von Datenobjekten des Dienstbetreibers mit ein, wobei eine durch die gematik vorgegebene Klassifizierung übernommen werden soll.

G3.2 - Definieren und Schützen von Assets

Als Assets werden z. B. Texte, Programme und Daten bezeichnet. Objekte, die einer bestimmten Person oder Gruppe gehören, werden als Benutzerassets bezeichnet. Bei Objekten, die bestimmten Systemservices oder Funktionen zugeordnet sind, spricht man von Betriebssystemassets. Als Betriebssystemassets werden die Datenobjekte bezeichnet, die Bestandteil folgender Systemkomponenten sind:

- Systemkontrollprogramm sowie die zugehörigen Mechanismen für die Zugriffskontrolle
- Subsysteme und Lizenzprogramme

Definieren und Schützen von Assets	
Grundlegende Aufgabenbereiche **Verantwortungen (P = Performt, A = Assist)**	**Dienstbetreiber**
Installieren, Pflegen und Erweitern neuer oder vorhandener Software zur Datenzugriffskontrolle (im Bedarfsfall), sofern Dienstbetreiber die Notwendigkeit dieser Software in seinem Sicherheitskonzept identifiziert hat [A_03324]	P
Implementieren der Funktionen und Merkmale der Zugriffskontrollsoftware, die die im vorliegenden Dokument definierten Anforderungen des spezifischen Dienstes in Bezug auf die geltenden Sicherheitsverfahren erfüllen [A_03325]	P

G3.2.1 - Klassifizierung von Assets und Datenobjekten

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 7.2.1 Classification guidelines (Richtlinien für die Einstufung).

[…]

Softwareverwaltung

[…]

Sicherheitsprobleme entwickeln sich oft über einen längeren Zeitraum und müssen deshalb retrospektiv analysierbar sein, indem sie z.B. in der Produktions-Referenzumgebung nachgestellt werden. Vereinfachend darf angenommen werden, dass Sicherheitsprobleme kaum von Produktionsdaten, sehr wohl aber von Konfigurationsdaten und Softwareständen abhängen.

~~Deshalb MÜSSEN Konfigurationsdaten und Softwarestände über einen Zeitraum von 3 Monate auf Tagesbasis und über einen Zeitraum von 10 Jahren auf Monatsbasis nachvollziehbar und wieder herstellbar sein [A_03328].~~

Deshalb MÜSSEN Systemzustände (Konfigurationsdaten und Softwarestände) der letzten 2 Jahre durch geeignete Dokumentation lückenlos nachvollziehbar sein [A_54408].

Systemzustände der letzten 30 Tage müssen sich (zur Nachstellung im Fehlerfall) wiederherstellen lassen [A_54409]

Im Einzelfall können mit dem Dienstbetreiber im SLA Werte vereinbart werden, die über die aufgeführten Werte hinausgehen.

Zur Beurteilung, ob festgestellte Abweichungen oder Änderungen geplant sind oder einen Sicherheitsvorfall darstellen, MÜSSEN Konfigurationsänderungen vollständig dokumentiert sein. Der Zugriff muss sowohl chronologisch als auch über den Namen der Komponente jederzeit möglich sein [A_03329].

Klassifizierung von Datenobjekten und Assets	**Verbindlicher Wert**
Klassifizierung von Datenobjekten durch den Dienstbetreiber [A_54411]	~~Nicht erforderlich~~ Verantwortung liegt bei Dienstbetreiber, Klassifizierung muss durch diesen vorgenommen werden
~~Verantwortung für die~~ Klassifizierung von Datenobjekten [A_54410]	~~gematik~~ Eine von der gematik vergebene Klassifizierung soll übernommen werden
Verantwortlich für die Klassifizierung von Assets [A_03332]	Dienstbetreiber

G3.2.8 - Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03324		S	Schutz_von_Assets_01: Installieren, Pflegen und Erweitern neuer oder vorhandener Software zur Datenzugriffskontrolle.	Grundlegender Aufgabenbereich (Dienstbetreiber performt): Der Dienstbetreiber MUSS neue oder vorhandene Software zur Datenzugriffskontrolle (im Bedarfsfall) installieren, pflegen und erweitern, wenn er die Notwendigkeit dieser Software in seinem Sicherheitskonzept identifiziert hat.		Anhang G 3.2
~~A_03328~~ *Ersetzt durch A_54408 A_54409*		~~S~~	~~Schutz_von_Assets_05: Nachvollziehbarkeit und Wiederherstellbarkeit von Konfigurationsdaten.~~	~~Konfigurationsdaten und Softwarestände MÜSSEN über einen Zeitraum von 3 Monaten auf Tagesbasis und über einen Zeitraum von 10 Jahren auf Monatsbasis nachvollziehbar und wieder herstellbar sein~~		~~Anhang G 3.2~~
A_54408		S		Der Betreiber MUSS die Dokumentation der Systemzustände (Konfigurationsdaten und Softwarestände) der letzten 2 Jahre lückenlos nachweisen.		Anhang G 3.2
A_54409		S		Der Betreiber MUSS Systemzustände (Konfigurationsdaten und Softwarestände) für die letzten 30 Tage (zur Nachstellung im Fehlerfall) wiederherstellen können.		Anhang G 3.2
~~A_03330~~ A_54410		S	Schutz_von_Assets_07: Klassifizierung von Datenobjekten durch den Dienstbetreiber.	Eine von der gematik vorgegebene Klassifikation von Datenobjekten SOLL vom Dienstanbieter übernommen werden.		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
~~A_03331~~ A_54411		S	Schutz_von_Assets_08: Verantwortung für die Klassifizierung von Datenobjekten	Der Betreiber MUSS die Klassifizierung von Datenobjekten durchführen und verantworten.		Anhang G 3.2