SRQ - Specification Related Question

SRQ-ID: 1171

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Trennung von Produktions- und Testumgebung
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 3.2.4, 3.2.8

Stichwort: Trennung von Produktions- und Testumgebung

Frage:

Ist eine virtuelle Trennung der Produktiv- und Testumgebungen möglich, obwohl die Anforderungen in gemSiKo#AnhG eine physikalische Trennung fordern (siehe SRQ 1044 für SiKo V 2.4.0 des Rel. 2.3.4)?

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:

Ja, auch eine virtuelle Trennung ist möglich, wenn hierdurch eine äquivalente Maßnahmenstärke erreicht wird.

In [gemSiKo] V2.4.0 wir das Kapitel „G3.2.4 – Produktivumgebungen“ mit den Anforderungen [A_04256 bis A_04262] eingeführt, um die in Kapitel „G3.2.5 Testumgebung“ (vormals G3.2.4 in [gemSiKo] V2.2.0) beschriebene Betriebsumgebungen ohne Echtdaten besser von der Betriebsumgebung mit Echtdaten abzugrenzen. In SRQ 1044 zu [gemSiKo] V2.4.0 wird die Frage

nach einer virtuellen Trennung dieser Betriebsumgebungen beantwortet und die Anforderung [A_03354] durch die Anforderungen [A_51336, A_51337] ersetzt.

Um die Möglichkeit einer virtuellen Trennung der Betriebsumgebungen auch in [gemSiKo] V2.2.0 zu beschreiben wird [gemSiKo] V2.2.0 um das entsprechende Kapitel mit den Anforderungen [A_04256 bis A_04262] ergänzt und das Kapitel „G3.2.4 Testumgebung“ in der folgenden Weise geteilt und um die notwendigen Änderungen angepasst.

G3.2.4.1 Betriebsumgebungen mit Echtdaten

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 10.1.4 Separation of development, test, and operational facilities.

Die Telematikinfrastruktur wird in mehreren getrennten Betriebsumgebungen mit unterschiedlichen Verwendungszwecken und Nutzern betrieben.

Aufbau und Betrieb des Dienstes MÜSSEN soweit organisatorisch, physisch oder logisch voneinander getrennt werden, dass Wechselwirkungen zwischen den Betriebsumgebungen ausgeschlossen werden können. Der Grad der Abgrenzung zwischen den Betriebsumgebungen MUSS im Sicherheitskonzept des Betreibers identifiziert und mit angemessenen Maßnahmen umgesetzt werden [A_04256].

Werden Software und Systemdaten zwischen Betriebsumgebungen mit Echtdaten überführt, so MÜSSEN die Regeln für die Überführung definiert und dokumentiert sein [A_04259]. Ferner MUSS der Dienstbetreiber sicherstellen, dass produktive Daten, insbesondere personenbezogene Daten (Echtdaten), nicht außerhalb der für sie bestimmten Betriebsumgebung zum Einsatz kommen [A_04260].

Werden in einer Betriebsumgebung Testdaten verwendet, MÜSSEN Daten verwendet werden, die keine Informationen enthalten, die auf echte Personen rückführbar sind, aber strukturell und inhaltlich Echtdaten so weit wie möglich gleichen, um Testergebnisse nicht zu verfälschen [A_04261].

Der Umgang mit kryptographischen Identitäten in Betriebsumgebungen mit Echtdaten MUSS im Sicherheitskonzept beschrieben sein [A_04262].

G3.2.4.2 Betriebsumgebungen ohne Echtdaten ~~Testumgebung~~

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 10.1.4 Separation of development, test, and operational facilities.

Betriebsumgebungen ohne Echtdaten sind vom Dienstbetreiber (normalerweise optional) unterhaltene Betriebsumgebungen, die der Entwicklung und dem Test von Software dienen, bevor diese in den Wirkbetrieb übernommen wird.

~~Die Stufe der Aufteilung zwischen Produktions-, Produktionsreferenz- und Testumgebung, welche notwendig ist, um Probleme in der Produktion zu verhindern, müssen im Sicherheitskonzept des Betreibers identifiziert und mit angemessenen Maßnahmen umgesetzt werden. Sie sind bis auf das MPLS physisch zu trennen [A_03354].~~

Der Betreiber SOLL Betriebsumgebungen mit Echtdaten von Betriebsumgebungen ohne Echtdaten physisch trennen, um Wechselwirkungen zwischen den Systemen zu minimieren [A_51336].

Die folgenden Punkte müssen beachtet werden:

- Der Betreiber MUSS die Äquivalenz der trennenden Maßnahmen bezüglich des Ausschlusses von Wechselwirkungen zwischen den Betriebsumgebungen in seinem Sicherheitskonzept nachweisen, wenn keine physische Trennung zwischen Betriebsumgebungen mit Echtdaten und Betriebsumgebungen ohne Echtdaten umgesetzt wird [A_51337].
- Der Umgang mit kryptographischen Identitäten im Testsystem MUSS im Sicherheitskonzept beschrieben sein [A_03355].
- Regeln für die Überführung von Software aus dem Entwicklungs- in den Produktionsstatus MÜSSEN definiert und dokumentiert sein [A_03356].
- Compiler, Editoren und andere Entwicklungs- oder Systemwerkzeuge DÜRFEN für produktive Systeme nicht im Zugriff liegen [A_03357].
- Die Testumgebung SOLL das Produktionssystem so exakt wie möglich nachbilden [A_03358].
- Benutzer SOLLEN unterschiedliche Benutzerprofile für Produktions- und Testsysteme haben, Menüs SOLLEN entsprechende Identifikationsmeldungen darstellen, um das Risiko von Fehlern zu reduzieren. Auch Kennungen für Wartungsfirmen und Servicepersonal sind auf beiden Systemen unterschiedlich zu gestalten [A_03359].
- Die folgenden Richtlinien MÜSSEN zum Schutz von Produktivdaten angewendet werden, wenn diese zu Testzwecken genutzt werden [A_03360]:
  - Wenn personenbezogene oder andere sensible Informationen zu Testzwecken verwendet werden, MÜSSEN alle sensiblen Inhalte entfernt oder so stark verändert werden, dass eine Wiedererkennung nicht mehr möglich ist [A_03361].
  - Alle für Produktivsysteme geltenden Maßnahmen zum Schutz der Vertraulichkeit der Informationen- insbesondere auch Zugangkontrollverfahren, die auf operativen Anwendungssysteme anwendbar sind, MÜSSEN ebenfalls auf Testanwendungssystemen angewendet werden [A_03362].
  - Es MUSS jedes Mal eine gesonderte Genehmigung notwendig sein, wenn Produktivdaten auf ein Testanwendungssystem kopiert werden [A_03363].
  - Produktivdaten MÜSSEN sofort von einem Testanwendungssystem gelöscht werden, nachdem das Testen abgeschlossen wurde [A_03364].
  - Das Kopieren und Verwenden von Echtdaten zu Testzwecken MUSS protokolliert werden [A_03365].

G3.2.8 - Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_04256		S		Aufbau und Betrieb des Dienstes MÜSSEN soweit organisatorisch, physisch oder logisch voneinander getrennt werden, dass Wechselwirkungen zwischen den Betriebsumgebungen ausgeschlossen werden können. Der Grad der Aufteilung zwischen den Betriebsumgebungen MUSS im Sicherheitskonzept des Betreibers identifiziert und mit angemessenen Maßnahmen umgesetzt werden.		Anhang G 3.2
A_04259		S		Regeln für die Überführung von Software und Systemdaten zwischen den Betriebsumgebungen mit Echtdaten MÜSSEN definiert und dokumentiert sein.		Anhang G 3.2
A_04260		S		Der Dienstbetreiber MUSS sicherstellen, dass produktive Daten insbesondere personenbezogene Daten (Echtdaten) nicht außerhalb der für sie bestimmten Betriebsumgebung zum Einsatz kommen.		Anhang G 3.2
A_04261		S		Werden in einer Betriebsumgebung Testdaten verwendet, MÜSSEN Daten verwendet werden, die keine Informationen enthalten, die auf echte Personen rückführbar sind, aber strukturell und inhaltlich Echtdaten so weit wie möglich gleichen, um Testergebnisse nicht zu verfälschen.		Anhang G 3.2
A_04262		S		Der Umgang mit kryptographischen Identitäten in Betriebsumgebungen mit Echtdaten MUSS im Sicherheitskonzept		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
				beschrieben sein.		
~~A_03354~~ *Ersetzt durch A_51336 A_51337*		~~S~~	~~Testumgebung_01: Trennung von Produktions-, Produktionsreferenz- und Testumgebung.~~	~~Die Stufe der Aufteilung zwischen Produktions-, Produktionsreferenz- und Testumgebung, welche notwendig ist, um Probleme in der Produktion zu verhindern, MÜSSEN im Sicherheitskonzept des Betreibers identifiziert und mit angemessenen Maßnahmen umgesetzt werden. Sie sind bis auf das MPLS physisch zu trennen.~~		~~Anhang G 3.2~~
A_51336		S		Der Betreiber SOLL Betriebsumgebungen mit Echtdaten von Betriebsumgebungen ohne Echtdaten physisch trennen, um Wechselwirkungen zwischen den Systemen zu minimieren.		Anhang G 3.2
A_51337		S		Der Betreiber MUSS die Äquivalenz der trennenden Maßnahmen bezüglich des Ausschlusses von Wechselwirkungen zwischen den Betriebsumgebungen in seinem Sicherheitskonzept nachweisen, wenn keine physische Trennung zwischen Betriebsumgebungen mit Echtdaten und Betriebsumgebungen ohne Echtdaten umgesetzt wird.		Anhang G 3.2
A_03355		S	Testumgebung_02: Umgang mit kryptographischen Identitäten im Testsystem.	Der Umgang mit kryptographischen Identitäten im Testsystem MUSS im Sicherheitskonzept beschrieben sein.		Anhang G 3.2
A_03356		S	Testumgebung_03: Regeln für die Überführung von Software aus dem Entwicklungs- in den Produktionsstatus.	Regeln für die Überführung von Software aus dem Entwicklungs- in den Produktionsstatus MÜSSEN definiert und dokumentiert sein.		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03357		S	Testumgebung_04: Entwicklungs- oder Systemwerkzeuge	Compiler, Editoren und andere Entwicklungs- oder Systemwerkzeuge DÜRFEN für produktive Systeme nicht im Zugriff liegen.		Anhang G 3.2
A_03358		S	Testumgebung_05: Die Testumgebung SOLL das Produktionssystem so exakt wie möglich nachbilden.	Die Testumgebung SOLL das Produktionssystem so exakt wie möglich nachbilden		Anhang G 3.2
A_03359		S	Testumgebung_06: Benutzerprofile und Menüs in Testumgebungen.	Benutzer SOLLEN unterschiedliche Benutzerprofile für Produktions- und Testsysteme haben, Menüs SOLLEN entsprechende Identifikationsmeldungen darstellen, um das Risiko von Fehlern zu reduzieren. Auch Kennungen für Wartungsfirmen und Servicepersonal sind auf beiden Systemen unterschiedlich zu gestalten.		Anhang G 3.2
A_03360		S	Testumgebung_07: Schutz von Produktivdaten.	Die folgenden Richtlinien [Testumgebung_08 - Testumgebung_12] MÜSSEN zum Schutz von Produktivdaten angewendet werden, wenn diese zu Testzwecken genutzt werden		Anhang G 3.2
A_03361		S	Testumgebung_08: Nutzung von personenbezogenen oder anderen sensiblen Informationen zu Testzwecken.	Wenn personenbezogene oder andere sensible Informationen zu Testzwecken verwendet werden, MÜSSEN alle sensiblen Inhalte entfernt oder so stark verändert werden, dass eine Wiedererkennung nicht mehr möglich ist.		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03362		S	Testumgebung_09: Zugangkontrollverfahren auf Testanwendungssystemen.	Alle für Produktivsysteme geltenden Maßnahmen zum Schutz der Vertraulichkeit der Informationen- insbesondere auch Zugangkontrollverfahren, die auf operativen Anwendungssysteme anwendbar sind, MÜSSEN ebenfalls auf Testanwendungssystemen angewendet werden.		Anhang G 3.2
A_03363		S	Testumgebung_10: Genehmigung zur Nutzung von Produktivdaten auf Testsystemen.	Es MUSS jedes Mal eine gesonderte Genehmigung notwendig sein, wenn Produktivdaten auf ein Testanwendungssystem kopiert werden.		Anhang G 3.2
A_03364		S	Testumgebung_11: Löschung der Produktivdaten vom testsystem unmittelbar nach Testende.	Produktivdaten MÜSSEN sofort von einem Testanwendungssystem gelöscht werden, nachdem das Testen abgeschlossen wurde;		Anhang G 3.2
A_03365		S	Testumgebung_12: Protokollierung des Transfers von Produktivdaten auf Testsysteme.	Das Kopieren und Verwenden von Produktivdaten in Testsysteme MUSS protokolliert werden.		Anhang G 3.2