SRQ - Specification Related Question

SRQ-ID: 1165

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Fehlende Anforderungen trotz normativem Fließtext
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 2.3, 3.1.3, 3.2.8, 3.3.2, 5.6, 6.2, 11.4

Stichwort: Fehlende Anforderungen trotz normativem Fließtext

Frage:

In [gemSiKo] sind im Anhang G im Fließtext Anforderungen formuliert, die nicht in den Tabellen der Zusammenfassungen der Sicherheitsanforderungen zu finden sind. Sind diese Anforderungen verbindlich?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	keine Zulassungsrelevanz		
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, der Fließtext des Anhang G ist normativ und somit verbindlich. Zur Erleichterung der Übersicht wurden die fehlenden Anforderungen identifiziert, Anforderungs-IDs vergeben und die Anforderungen in den Tabellen der Zusammenfassungen der Sicherheitsanforderungen der jeweiligen Kapitel des Anhangs G aufgenommen.

G2.3 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54395		S		Der Betreiber MUSS physische Zugangskontrollen einrichten, um Risiken wie Diebstahl oder Beschädigung der Systeme für die Informationsverarbeitung, nicht autorisierte Weitergabe oder Löschung von Informationen sowie die Unterbrechung der Unterstützung für Geschäftsprozesse und potenzielle Datenverluste zu vermeiden.		Anhang G 2

G3.1.3 – Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54396		S		Der Betreiber MUSS sicherstellen, dass jedem potenziellen Benutzer des Systems eine eindeutige Kennung (z. B. eine Benutzer-ID) zugeordnet werden kann.		Anhang G 3.1
A_54397		S		Wenn sich der Benutzer am System anmeldet, MUSS durch eine weitere Identifikationsstufe (z. B. ein Kennwort) sichergestellt werden, dass der Benutzer die Person ist, für die er sich ausgibt.		Anhang G 3.1
A_54398		S		Der Betreiber MUSS sicherstellen, dass jede Ressource auf dem System identifiziert werden kann.		Anhang G 3.1

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54399		S		Der Betreiber MUSS sicherstellen, dass der Zugriff auf jede Ressource des Systems nur im definierten Umfang für autorisierte Benutzer gewährt und für nicht autorisierte Benutzer verweigert wird.		Anhang G 3.1
A_54400		S		Der Betreiber MUSS sicherstellen, dass die Sicherheitsfunktionen des Systems nur von autorisierten Benutzern definiert, geändert oder deaktiviert werden können.		Anhang G 3.1
A_54401		S		Der Betreiber MUSS sicherstellen, dass für jeden erfolgreichen oder fehlgeschlagenen Zugriffsversuch auf das System oder auf geschützte Assets innerhalb des Systems ein Protokolleintrag erstellt wird.		Anhang G 3.1
A_54402		S		Der Betreiber MUSS sicherstellen, dass nicht autorisierte Zugriffsversuche auf Systeme oder Informationen durch sofortige oder spätere Analysen als Zugriffsverletzungen erkannt werden.		Anhang G 3.1
A_54403		S		Der Betreiber MUSS einen Prozess für die Berechtigungen von Benutzern für den Zugriff auf die verfügbaren Computersysteme implementieren.		Anhang G 3.1
A_54404		S		Innerhalb des Autorisierungsprozesses der Berechtigungen einer Benutzer-ID MUSS der Manager des Benutzers benachrichtigt werden.		Anhang G 3.1
A_54405		S		Auf Clustersystemen SOLLEN Benutzer-IDs nur für den Zugriff auf das Systemcluster und nicht für den Zugriff auf jeden einzelnen Knoten des Clusters eingerichtet werden. *Zur Beachtung: Der Anforderungstext wird durch den SRQ 1161 geändert:*		Anhang G 3.1

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
				Auf Clustersystemen SOLLEN Benutzer-IDs nur für den Zugriff auf das Systemcluster und nicht für den Zugriff auf jeden einzelnen Knoten des Clusters erneut überprüft werden.		
A_54428		S		Wenn ein Benutzer aus dem Unternehmen ausscheidet, sich beurlauben lässt und nicht erwartet wird, dass er wieder in ein reguläres Beschäftigungsverhältnis eintritt oder wenn für ihn kein gültiger geschäftlicher Grund mehr vorliegt, auf bestimmte Daten zugreifen zu können, MUSS der zuständige Manager den bzw. die für die Benutzer-ID zuständigen Administrator(en) hierüber informieren.		Anhang G 3.1
A_54429		S		Die für die Benutzer-ID zuständigen Administratoren MÜSSEN über einen Prozess oder technische Kontrollmechanismen verfügen, um sofort nach der Managementbenachrichtigung über einen ausgeschiedenen oder beurlaubten Benutzer den Zugriff des betreffenden Benutzers auf die Systeme zu unterbinden.		Anhang G 3.1
A_54430		S		Versetzen von Mitarbeitern an einen anderen Standort oder in einen anderen Bereich: Löschung erst erforderlich, wenn der geschäftliche Grund erlischt *Zur Beachtung: Der Anforderungstext wird durch den SRQ 1161 geändert:* Wenn der geschäftliche Grund für die Existenz einer Benutzer-ID erloschen ist (z. B. nachdem ein Mitarbeiter an einen anderen Standort oder in einen anderen Bereich versetzt wurde), MUSS der Betreiber die betreffende Benutzer-ID löschen		Anhang G 3.1

G3.2.8 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54407		S		Der Betreiber MUSS alle Assets identifizieren und die Wichtigkeit dieser Assets dokumentieren.		Anhang G 3.2
A_54413		S		Die Integrität von Betriebssystemassets MUSS durch das Definieren entsprechender Optionen für den Zugriffsschutz gewährleistet werden. Veränderungen an Betriebssystemassets MÜSSEN durch regelmäßige Integritätsprüfungen entsprechend des Schutzbedarfes verarbeiteter Datenobjekte erkannt werden. Der Betreiber MUSS die Verfahren im Sicherheitskonzept dokumentieren.		Anhang G 3.2
A_54415		S		Wenn ein System oder Server mit einem Computervirus infiziert wurde, MUSS der Systemadministrator sich an die zuständige, vom Dienstbetreiber vorgesehene Servicefunktion wenden, um den durch den Virus verursachten Schaden auf ein Minimum zu begrenzen.		Anhang G 3.2

G3.3.2 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54416		S		Der Betreiber MUSS für die Genehmigung und Gewährung von privilegierten Berechtigungen einen Prozess implementieren.		Anhang G 3.3

G5.6 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54417		S		Der Betreiber MUSS vor der Entsorgung von Speichermedien oder deren Weiterverwendung durch andere Kunden die Restdaten unlesbar machen. Dabei MÜSSEN die Vorgaben des BSI beachtet werden. Die Klassifizierung der Medien MUSS im Sicherheitskonzept beschrieben werden.		Anhang G 5

G6.2 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54418		S		Der Dienstbetreiber ist verpflichtet, alle beobachteten oder vermuteten Sicherheitsschwachstellen in Systemen oder Services zu notieren und zu melden.		Anhang G 6

G11.4 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54422		S		Der Betreiber DARF NICHT Fernanmeldungen von root/Administrator Benutzern auf Firewallsystemen erlauben.		Anhang G 11