SRQ - Specification Related Question

SRQ-ID: 1161

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Benutzer-IDs und Passworte
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 3.1.1, 3.1.2, 3.1.3

Stichwort: Benutzer-IDs und Passworte

Frage:

Anforderung [A_03277] fordert, dass Benutzer-IDs nur dem Benutzer selbst bekannt sind, dennoch ist eine Verwendung der Benutzer-ID als Kennwort durch Anforderung [A_03303] verboten. Wie können Benutzer-IDs unter diesen Maßgaben überprüft und ggf. gesperrt/gelöscht werden? Sind Benutzer-IDs, die gemeinsam von einer Gruppe genutzt werden, umzubenennen wenn ein Benutzer die Gruppe verläßt (siehe Anforderung [A_03279])? Müssen Benutzer-IDs wie Kennworte als Hash-Wert gespeichert werden (siehe Anforderung [A_03311])?

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:

Die Anforderungen an die Nutzung von Benutzer-IDs, auch im Kontext der Nutzung durch eine Gruppe von Benutzern, ist an mehreren Stellen geschärft worden. Insbesondere ist die Forderung, dass eine Benutzer-ID nur dem Eigner bekannt sein darf, aufgehoben worden und die Nutzung der Benutzer-ID als Teil des Kennworts ist überarbeitet worden. Die Anforderungen und die

Speicherung von Kennworten sind im Zuge dieser Überarbeitung ebenfalls klarer formuliert worden.

G3.1.1 - Benutzer-IDs

Entsprechende Anforderungen gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 11.2.1 User registration (Anmeldung von Benutzern) und Ziffer 11.5.2 User identification and authentication (Benutzeridentifikation und -authentisierung).

Die Zugriffsberechtigungen für die Systeme MÜSSEN auf der Basis der aktuellen geschäftlichen Notwendigkeiten vergeben und durch die Überprüfung der Identität von Benutzern und Anwendungen kontrolliert werden [A_03275]. Benutzer-IDs MÜSSEN einer bestimmten Person eindeutig zugeordnet werden können [A_03276]. Dazu MUSS jedem Benutzer eine eindeutige Benutzer-ID und ein geheimer Code (z. B. ein Kennwort) zugewiesen werden, wobei der geheime Code nur dem Eigner der Benutzer-ID bekannt ist. Die hier beschriebenen Benutzer-IDs sind die IDs für die Anmeldung am System bzw. Server [A_03277].

Wenn im Sicherheitskonzept eine SmartCard oder andere, stärkere Credentials zur Authentifizierung von Benutzern gefordert wird, hat diese Forderung Vorrang vor den im Weiteren gemachten Vorgaben.

Verwendung einer Benutzer-ID durch eine Gruppe [A_03278]:

- Die Verwendung einer Benutzer-ID durch eine Gruppe stellt grundsätzlich ein Risiko da. Die Notwendigkeit MUSS jeweils im Sicherheitskonzept begründet werden und es MUSS dargelegt werden, wieso die Sicherheit des Systems dadurch nicht unzulässig reduziert wird.

Unter folgenden Bedingungen DÜRFEN Benutzer-IDs bzw. Kennwörter von einer Gruppe gemeinsam verwendet werden:

- Die Software lässt die Verwaltung persönlicher Zugriffsaccounts nicht zu und spezielle Benutzer-IDs oder Kennwörter sind für den Zugriff auf Funktionen, die von einer bestimmten Personengruppe bzw. Rolle benötigt werden, unbedingt erforderlich.
- Die nicht autorisierte Verwendung der Benutzer-ID oder des Kennworts MUSS verhindert werden.
- Der Zugriff MUSS nur auf die Funktionen eingeschränkt werden, die für die Gruppe genehmigt sind.
- Alle Mitglieder der Gruppe MÜSSEN für die Daten zugriffsberechtigt sein, für die die Benutzer-ID zugriffsberechtigt ist.
- Die Zuordnung welche individuellen Benutzer zu einem bestimmten Zeitpunkt einer Benutzer-ID zugeordnet waren, MUSS sich aus manuell geführten Kontrollblättern nachvollziehen lassen.

[…]

Berechtigung von Benutzer-IDs

[…]

Berechtigung von Benutzer-IDs	Verbindlicher Wert
[…] Als Cluster verwaltete Systeme	[…] Benutzer-IDs SOLLEN nur für den Zugriff auf das Systemcluster und nicht für den Zugriff auf jeden einzelnen Knoten des Clusters eingerichtet werden [A_54405]

Überprüfung des Beschäftigungsverhältnisses

[…]

Überprüfung des Beschäftigungsverhältnisses	Verbindlicher Wert
[…] Geschäftlicher Grund für die Existenz einer Benutzer-ID erloschen (z. B. nachdem ein Mitarbeiter an einen anderen Standort oder in einen anderen Bereich versetzt wurde) [A_54430]	[…] Betreiber MUSS die betreffende Benutzer-ID löschen

[…]

Erneute Überprüfung (Revalidierung) von Benutzer-IDs auf Vorliegen eines geschäftlichen Grundes

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 11.2.4 Review of user access rights (Überprüfung der Zugriffsrechte der Benutzer).

Für die erneute Überprüfung (Revalidierung) von Benutzer-IDs MUSS ein dokumentierter Prozess implementiert werden. Im Rahmen dieser erneuten Überprüfung MÜSSEN alle Benutzer-IDs des Dienstbetreibers überprüft werden. Darüber hinaus MUSS festgestellt werden, ob noch ein gültiger geschäftlicher Grund für die Zugriffsberechtigung des Benutzers auf das jeweilige System vorliegt. Benutzer, deren geschäftlicher Grund für den Systemzugriff erloschen ist, MÜSSEN zwecks Löschung ihrer ID dem für die Benutzer-ID zuständigen Administrator gemeldet werden. Die Löschungen MÜSSEN mit Zeit und Grund dokumentiert werden.

Die erneute Überprüfung KANN in Form eines Berichts an das zuständige Management realisiert werden, in dem alle Mitarbeiter aufgeführt sind, die über eine Zugriffsberechtigung für das System verfügen. Das Management MUSS hierbei festgestellte Abweichungen weiterverfolgen und mit dem für die Benutzer-ID zuständigen Administrator abklären. Die erstellten Berichte KÖNNEN wieder zurückgegeben werden [A_03294].

[…]

G3.1.2 - Kennwörter

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 11.2.3 User password management (Verwaltung von Benutzerpasswörtern) und Ziffer 11.5.3 Password management system (Kennwortverwaltungssystem).

Kennwörter können zur Authentisierung von Benutzern verwendet werden. Die Zuverlässigkeit des gewählten Kennworts ist der wichtigste Faktor für den Schutz von Systemen und Anwendungen. Die Regeln für das Definieren von Kennwörtern, die im vorliegenden Abschnitt erläutert werden, gelten für alle Kennwörter, die für die Anmeldung an den verfügbaren Systemen und Subsystemen eingesetzt werden.

Kennwörter	Verbindlicher Wert	Anforderungen des spezifischen Dienstes
[…]	[…]	
Benutzer-ID oder eine Permutation ihrer Zeichen im Kennwort	DARF NICHT als Teilzeichenkette Bestandteil des Kennwortes sein [A_54406]	
[…]	[…]	

Hinweis: Bestimmte Benutzer-IDs müssen über Kennwörter ohne Ablaufdatum verfügen. Diese Ausnahmen sind im Betriebskonzept des Dienstbetreibers beschrieben.

Schutz von Kennwörtern

Schutz von Kennwörtern	Mindestanforderung
[…] Kennwortspeicherung	[…] Bei der Speicherung zum Zwecke der späteren Validierung im Zuge einer Authentifizierung MUSS das Kennwort in Form seines Hashwertes gespeichert werden [A_03311]

G3.1.3 – Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03277		S	Benutzer_IDs_03: Eindeutige Zuordnung des geheimen Codes.	Jedem Benutzer muss eine eindeutige Benutzer-ID und ein geheimer Code (z. B. ein Kennwort) zugewiesen werden, wobei der geheime Code nur dem Eigner der Benutzer-ID bekannt ist. Die hier beschriebenen Benutzer-IDs sind die IDs für die Anmeldung am System bzw. Server.		Anhang G 3.1
A_03278		S	Benutzer_IDs_04: Verwendung einer Benutzer-ID durch eine Gruppe	Die Verwendung einer Benutzer-ID durch eine Gruppe stellt grundsätzlich ein Risiko da. Die Notwendigkeit MUSS jeweils im Sicherheitskonzept begründet werden und es MUSS dargelegt werden, wieso die Sicherheit des Systems dadurch nicht unzulässig reduziert wird. Unter folgenden Bedingungen DÜRFEN Benutzer-IDs bzw. Kennwörter von einer Gruppe gemeinsam verwendet werden: • Die Software lässt die Verwaltung persönlicher Zugriffsaccounts nicht zu und spezielle Benutzer-IDs oder Kennwörter sind für den Zugriff auf Funktionen, die von einer bestimmten Personengruppe bzw. Rolle benötigt werden, unbedingt erforderlich. • Die nicht autorisierte Verwendung der Benutzer-ID oder des Kennworts MUSS verhindert werden. • Der Zugriff MUSS nur auf die Funktionen eingeschränkt werden, die für die Gruppe genehmigt sind. • Alle Mitglieder der Gruppe MÜSSEN für die Daten zugriffsberechtigt sein, für die die Benutzer-ID zugriffsberechtigt ist. • Die Zuordnung welche individuellen Benutzer zu einem bestimmten Zeitpunkt einer Benutzer-ID zugeordnet waren, MUSS sich aus manuell geführten Kontrollblättern nachvollziehen lassen.		Anhang G 3.1

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
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.		Anhang G 3.1
A_54430		S		Wenn der geschäftliche Grund für die Existenz einer Benutzer-ID erloschen ist, MUSS der Betreiber die betreffende Benutzer-ID löschen.		Anhang G 3.1
A_03294		S	Benutzer_IDs_20: Revalidierung der Benutzer-IDs.	Für die erneute Überprüfung (Revalidierung) von Benutzer-IDs MUSS ein dokumentierter Prozess implementiert werden. Im Rahmen dieser erneuten Überprüfung MÜSSEN alle Benutzer-IDs des Dienstbetreibers überprüft werden. Darüber hinaus MUSS festgestellt werden, ob noch ein gültiger geschäftlicher Grund für die Zugriffsberechtigung des Benutzers auf das jeweilige System vorliegt. Benutzer, deren geschäftlicher Grund für den Systemzugriff erloschen ist, MÜSSEN zwecks Löschung ihrer ID dem für die Benutzer-ID zuständigen Administrator gemeldet werden. Die Löschungen MÜSSEN mit Zeit und Grund dokumentiert werden. Die erneute Überprüfung KANN in Form eines Berichts an das zuständige Management realisiert werden, in dem alle Mitarbeiter aufgeführt sind, die über eine Zugriffsberechtigung für das System verfügen. Das Management MUSS hierbei festgestellte Abweichungen weiterverfolgen und mit dem für die Benutzer-ID zuständigen Administrator abklären. Die erstellten Berichte KÖNNEN wieder zurückgegeben werden.		Anhang G 3.1
~~A_03303~~ *Ersetzt durch A_54406*		~~S~~	~~Kennwörter_03: Komplexitätsanforderungen / Ausschlußkriterien.~~	~~Benutzer-ID im Kennwort; Nein~~		~~Anhang G 3.1~~
A_54406		S		Die Benutzer-ID oder eine Permutation ihrer Zeichen DARF NICHT als Teilzeichenkette Bestandteil des Kennwortes sein.		Anhang G 3.1

SRQ - Specification Related Question

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03311		S	Kennwörter_11: Kennwortspeicherung	Kennwortspeicherung: Bei der Speicherung zum Zwecke der späteren Validierung im Zuge einer Authentifizierung MUSS das Kennwort in Form seines Hashwertes gespeichert werden		Anhang G 3.1