SRQ - Specification Related Question

SRQ-ID: 1162

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Bewertung von Sicherheitsvorfällen
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 6., 6.2

Stichwort: Bewertung von Sicherheitsvorfällen

Frage:

Anforderung [A_03485] sieht als Analyseschritt eine Sichtung bzw. Milderung von Schäden im Falle eines Sicherheitszwischenfalls vor. Zu welchem Zeitpunkt werden Schäden bewertet um angemessene Maßnahmen zur Verminderung auszuwählen?

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:

Der Analyseschritt sieht ebenfalls eine Bewertung der Schäden vor. Der Text von Anforderung [A_03485] wurde dahingehend konkretisiert.

G6 - Management von Sicherheitszwischenfällen

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 13.1.1 Reporting information security events (Meldung sicherheitsrelevanter Ereignisse) und Ziffer 13.1.2 Reporting security weaknesses (Meldung von Sicherheitsschwachstellen).

Ein Sicherheitszwischenfall kann interne oder externe Ursachen haben, sich auf externe Standorte auswirken und in seiner Wertigkeit variieren. Als IT-Sicherheitszwischenfälle bezeichnet man u. a. Systemeinbrüche, die Zerstörung von Daten, Manipulationen, kriminelle Handlungen oder andere schwerwiegende Beeinträchtigungen der Systemsicherheit. Andere Zwischenfälle können in der Regel durch das zuständige Standortmanagement und das zugehörige Personal bearbeitet werden.

[…]

Melden von Sicherheitszwischenfällen	Verbindlicher Wert
[…] Analyse	[…] Sichten, Bewerten und Mitigieren ~~bzw. Mildern~~ der Schäden, die an den verfügbaren Assets und Daten zu verzeichnen sind [A_03485]

G6.2 – Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03485		S	Security_Incident_Management_05:Analyse: Sichten bzw. Mildern der Schäden	Der Dienstbetreiber MUSS Schäden, die an den verfügbaren Assets und Daten zu verzeichnen sind, sichten, bewerten und mitigieren.		Anhang G 6