SRQ - Specification Related Question

SRQ-ID: 1145

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	SD1-ISADM-006: Fehlender Sicherheitsmanagement-Prozess zum technischen Schwachstellenmanagement
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	8.1, 8.5a, 8.10

Stichwort: SD1-ISADM-006: Fehlender Sicherheitsmanagement-Prozess zum technischen Schwachstellenmanagement

Frage:

Gibt es innerhalb des Sicherheitsmanagements einen eigenständigen Prozess zum Schwachstellenmanagement?

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:	Dieser SRQ enthält Maßnahmen, die sich aus dem Sicherheitsgutachten ergeben haben.		
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Anforderung [A_02386], welche in der Anforderungstabelle in Kapitel 8.10 die Aufgaben des Sicherheitsmanagements beschreibt, wird um die „Ermittlung und Analyse von Schwachstellen“ ergänzt. Der entsprechende Text in Kapitel 8.1 „Begriffsbestimmung“ wird angepasst und ein neues Kapitel 8.5a wird aufgenommen, welches das technische Schwachstellenmanagement beschreibt.

8.1 Begriffsbestimmung

[…]

Zu den Aufgaben des Sicherheitsmanagements gehören:

- Festlegung der Sicherheitsziele, -strategien und –policies,
- Festlegung der Sicherheitsanforderungen,
- Ermittlung und Analyse von Schwachstellen, Bedrohungen und Risiken,
- Festlegung geeigneter Sicherheitsmaßnahmen,
- Überwachung der Implementierung und des laufenden Betriebes der selektierten Maßnahmen,
- Förderung des Sicherheitsbewusstseins sowie
- Detektion von und Reaktion auf sicherheitsrelevante Ereignisse. (Security Incident Management; dieses soll in das allgemeine Incident Management eingebettet sein, welches möglichst nach ITIL ~~eingebettet~~ausgerichtet werden soll).

[…]

8.5a Technisches Schwachstellenmanagement

Zur Aufrechterhaltung des notwendigen Sicherheitsniveaus im laufenden Betrieb muss jeder Betreiber, entsprechend der Vorgaben in Kapitel 8.5 und Anhang G7, sowohl einen Prozess zur Erkennung und Analyse von Schwachstellen als auch einen Prozess zur Bewertung und Implementierung von Sicherheitsupdates etablieren. Die jeweiligen Betreiber sind daher verpflichtet, die Sicherheitswarnungen der Hersteller der betriebenen Komponenten und Dienste, aber auch der sie unterstützenden Hard- und Software, zu beachten (vgl. ISO/IEC 27001, Anhang A.12.6).

Die gematik unterstützt diese Prozesse, indem sie zusätzlich Meldungen zu Schwachstellen und deren Gegenmaßnahmen in TI-spezifischen Komponenten und Diensten entgegennimmt, aufbereitet, TI-spezifisch bewertet, konsolidiert, und den Betreibern von Komponenten und Diensten bereitstellt bzw. (bei bislang unbekannten Schwachstellen) an die jeweiligen Hersteller weiterleitet. Die Betreiber sind aufgefordert, bislang unbekannte, selbst gefundene Schwachstellen an die gematik zu melden.

Die gematik koordiniert ferner die Weiterleitung von aufbereiteten, bewerteten und konsolidierten Sicherheitsmeldungen einzelner Betreiber, die andere Dienste beeinflussen oder Auswirkungen auf nicht von diesem Betreiber verantwortete Teile der Telematikinfrastruktur haben.

Durch Analyse der innerhalb des Schwachstellenmanagements gemeldeten Ereignisse können durch die gematik eigene Warnungen erstellt und an Betreiber oder Hersteller gemeldet werden.

Schwachstellen, die durch einen Betreiber im Rahmen seines Prozesses zur Bewertung und Implementierung von Sicherheitsupdates nicht behoben werden, müssen durch das Risikomanagement des Betreibers bewertet und behandelt werden. Die vom Betreiber bestimmten Restrisiken müssen an die gematik gemeldet und von dieser akzeptiert werden (siehe [A_02390] in Kapitel 8.10).

8.10 Zusammenstellung der Ausgangsanforderungen

Afo-ID	Art	Titel	Beschreibung	Rel.	Quelle
A_02386	S	Sec_Management_002: Aufgaben des Sicherheitsmanagements.	Das Sicherheitsmanagement sowohl der gematik als auch der Anbieter und Betreiber, die Teile der Telematikinfrastruktur verantworten, MUSS mindestens die folgende Aufgaben wahrnehmen: • Festlegung der Sicherheitsziele, -strategien und –policies, • Festlegung der Sicherheitsanforderungen, • Ermittlung und Analyse von Schwachstellen, Bedrohungen und Risiken, • Festlegung geeigneter Sicherheitsmaßnahmen, • Überwachung der Implementierung und des laufenden Betriebes der selektierten Maßnahmen, • Förderung des Sicherheitsbewusstseins sowie • Detektion von und Reaktion auf sicherheitsrelevante Ereignisse. (Security-incident-Management; dieses soll in das allgemeine Incident Management eingebettet sein, welches möglichst nach ITIL ~~eingebettet~~ausgerichtet werden soll).		Kap. 8
A_02390	S	Risikomanagemntprozess: Gestaltung des Risikomanagements.	Auf Basis der von der gematik festgelegten Mindeststandards MUSS jeder Betreiber innerhalb der Telematikinfrastruktur seinen eigenen Risikomanagementprozess gestalten, mittels dessen er Schwachstellen erkennt und durch Maßnahmen mindert, das Restrisiko bestimmt und die Verantwortung dafür übernimmt. Die vom Betreiber bestimmten Restrisiken müssen immer an die gematik gemeldet und von dieser akzeptiert werden		Kap. 8