SRQ - Specification Related Question

SRQ-ID: 1167

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Härtung und Verschlüsselung
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 3.2.5, 3.2.6, 3.2.8

Stichwort: Härtung und Verschlüsselung

Frage:

Gibt es konkrete Anforderung an die Härtung von Betriebssystemen und Konfiguration von Verschlüsselungsdiensten, die über die in den Anforderungen [A_03377 bis A_03379] beschriebenen Schlüssellängen hinausgehen?

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 Härtung von Betriebssystemen wird durch die neu erstellten Anforderungen [A_54485 bis A_54487] konkretisiert. Die Datenverschlüsselungsanforderungen können nun durch den Dienstbetreiber angepasst werden wobei die relevanten Dokumente gemSpec_Krypt und BSI TR-03116 angewendet werden müssen, in denen die übergreifenden Anforderungen umfassend beschrieben werden.

G3.2.5 - Betriebssystemassets

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 11.5.4 Use of system utilities (Gebrauch von Systemdienstprogrammen), Ziffer 12.4.1 Control of operational software (Kontrolle von Software in laufenden Systemen) und Ziffer 15.3.2 Protection of system audit tools (Schutz der Systemauditttools).

Die meisten Betriebssysteme sind standardmäßig auf maximale Kompatibilität statt optimaler Sicherheit konfiguriert. Die Konfiguration und Funktionalität eines durch den Dienstbetreiber eingesetzten Betriebssystemassets muss daher den Sicherheitsanforderungen entsprechend angepasst werden, um bekannten und zukünftigen Bedrohungen besser zu widerstehen („Härtung“).

Der Dienstbetreiber MUSS eine Anpassung der Konfiguration aller Sicherheitsfunktionen der Betriebssystemassets durchführen und dokumentieren [A_54485].

Der Dienstbetreiber SOLL alle nicht notwendigen Anwendungen und Komponenten des Betriebssystems entfernen [A_54486]. Ist die Entfernung einer derartigen Anwendungen oder Komponenten nicht möglich, so MUSS diese Anwendung oder Komponente deaktiviert werden [A_54487].

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. Die Verfahren sind im Sicherheitskonzept zu dokumentieren [A_54413].

[…]

3.2.6 - Verschlüsselung

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer entspricht Ziffer 11.5.3 Password management system (Kennwortverwaltungssystem) und Ziffer 12.3.1 Policy on the use of cryptographic controls (Policy für den Einsatz kryptographischer Maßnahmen).

[…]

Verschlüsselung		
Grundlegende Aufgabenbereiche **Verantwortungen (P = Performt, A = Assistiert)**	**Dienstbetreiber**	**gematik**
Definieren und Bereitstellen der übergreifenden Datenverschlüsselungsanforderungen des spezifischen Dienstes für Dienstbetreiber [A_03373]		P
Ableitung der spezifischen für die Betriebsumgebung relevanten Anforderungen auf Basis der übergreifenden Datenverschlüsselungsanforderungen [A_54414]	P	
[…]	[…]	[…]

Die umzusetzenden Standards bezüglich der Länge der Schüssel und der zulässigen Algorithmen sind im Kryptographiekonzept definiert, das von der gematik herausgegeben

wird. Darüber hinaus gelten folgende Anforderungen für den Einsatz von Schlüsseln, falls der Einsatzbereich nicht im Kryptographiekonzept thematisiert wird:

Verschlüsselung	Verbindlicher Wert
Aktivieren von Verschlüsselungsservices, die als integraler Bestandteil der Betriebssysteme, Subsysteme und Anwendungen implementiert sind [A_03376]	Ja
Geheime Chiffrierschlüssel (auch als symmetrische oder gemeinsame Schlüssel bezeichnet) [A_54607]	Entsprechend der Vorgaben aus [gemSpec_Krypt] und [BSI-TR-03116] ~~Mindestens 128 Bit Länge~~
Public/Private-Chiffrierschlüsselpaare (auch als asymmetrische oder duale Schlüssel bezeichnet) solange nicht ECC nach Vorgabe des Kryptokonzepts eingesetzt werden [A_03378]	Entsprechend der Vorgaben aus [gemSpec_Krypt] und [BSI-TR-03116] ~~Mindestens 1024 Bit Länge~~
Chiffrierschlüssel für die Übertragung vertraulicher Daten in öffentlichen Netzwerken, sofern nicht Stromverschlüsselung eingesetzt wird [A_03379]	Entsprechend der Vorgaben aus [gemSpec_Krypt] und [BSI-TR-03116] ~~Mindestens 128 Bit Länge~~

G3.2.8 - Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54485		S		Der Dienstbetreiber MUSS eine Anpassung der Konfiguration aller Sicherheitsfunktionen der Betriebssystemassets durchführen und dokumentieren.		Anhang G 3.2
A_54486		S		Der Dienstbetreiber SOLL alle nicht notwendigen Anwendungen und Komponenten des Betriebssystems entfernen.		Anhang G 3.2
A_54487		S		Ist die Entfernung einer nicht notwendigen Anwendung oder Komponente eines Betriebsystemes nicht möglich, so MUSS diese Anwendung oder Komponente deaktiviert werden.		Anhang G 3.2
A_03373		S	Verschlüsselung_03: Definieren und Bereitstellen der Datenverschlüsselungsanforderungen.	Die gematik MUSS die übergreifenden Datenverschlüsselungs-anforderungen des spezifischen Dienstes für Dienstbetreiber definieren und bereitstellen.		Anhang G 3.2
A_54414		S		Der Anbieter MUSS die spezifischen für die Betriebsumgebung relevanten Anforderungen auf Basis der übergreifenden Datenverschlüsselungsanforderungen ableiten.		Anhang G 3.2
~~A_03377~~ A_54638		S	Verschlüsselung_07:Mindestlänge geheime Chiffrierschlüssel	Die Länge von Chiffrierschlüsseln (auch als symmetrische oder gemeinsame Schlüssel bezeichnet) MÜSSEN den Vorgaben aus [gemSpec_Krypt] und [BSI-TR-03116] entsprechen.		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03378		S	Verschlüsselung_08: Mindestlänge von Public/Private-Chiffrierschlüsselpaaren.	Public/Private-Chiffrierschlüsselpaare (auch als asymmetrische oder duale Schlüssel bezeichnet) MÜSSEN den Vorgaben aus [gemSpec_Krypt] und [BSI-TR-03116] entsprechen.		Anhang G 3.2
A_03379		S	Verschlüsselung_09: Mindestlänge der Chiffrierschlüssel für die Übertragung vertraulicher Daten in öffentlichen Netzwerken.	Chiffrierschlüssel für die Übertragung vertraulicher Daten in öffentlichen Netzwerken MÜSSEN den Vorgaben aus [gemSpec_Krypt] und [BSI-TR-03116] entsprechen.		Anhang G 3.2