SRQ - Specification Related Question

SRQ-ID: 1172

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Virtualisierte Betriebssystemumgebungen
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 3.2

Stichwort: Virtualisierte Betriebssystemumgebungen

Frage:

SRQ 1171 erlaubt eine virtuelle Trennung von Betriebsumgebungen mit und ohne Echtdaten (vormals: Produktiv- und Testumgebungen), wenn hierdurch eine äquivalente Maßnahmenstärke erreicht wird. Welche Anforderungen werden generell an virtualisierte Betriebsumgebungen gestellt?

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		

(wird von der bearbeitenden AG ausgefüllt):

Antwort:

Kapitel G3.2 gemSiKo v2.2.0 wird um einen Abschnitt G3.2.4.3 mit den Anforderungen [A_54468 bis A_54484] ergänzt, der die Anforderungen an virtualisierte Betriebsumgebungen beschreibt

G3.2.4.3 Virtualisierte Betriebssystemumgebungen

Entsprechende Anforderung gemäß ISO/IEC 27002:2005
Diese Ziffer findet (noch) keine Berücksichtigung in ISO 27002:2005, da die Entwicklung der Virtualisierungstechnologien erst in den letzten Jahren eine weite Verbreitung und Anwendung in Rechenzentren gefunden haben.

Virtualisierungstechnologien erlauben den Betrieb mehrerer (virtueller) Maschinen auf einem einzelnen (physischen) Server. Dabei stellt der Virtual Machine Monitor (VMM) eine software-emulierte Hardware-Schnittstelle zur Verfügung. Der Zugriff einer virtuellen Maschine (Gast) auf diese Schnittstelle führt zu einem Zugriff auf die physische Hardware-Schnittstelle, was den Betrieb mehrerer virtualisierter (logisch getrennter) Betriebssystemumgebungen erlaubt.

Da bei einer rein logischen Isolation die physische Isolation der einzelnen Betriebssystemumgebungen verloren geht, führt dies immer zu einer Senkung des Sicherheitsniveaus. Konkret vergrößert sich die Trusted Computing Base (TCB) eines virtualisierten Systems mindestens um den aktuellen VMM (ggf. auch um die enthaltenen Treiber oder das komplette Betriebssystem, auf dem der VMM aufsetzt, oder alle VMM, auf denen das virtualisierte System jemals betrieben wurde). Es ist daher erforderlich, diese Absenkung auf ein akzeptables Maß zu reduzieren.

Sämtliche für reale Betriebssystemumgebungen definierten und implementierten Schutzmaßnahmen und Sicherheitsprozesse (oder nachweisliche äquivalente Maßnahmen bzw. Prozesse) MÜSSEN auch auf virtualisierte Betriebssystemumgebungen angewendet werden [A_54468].

Jede virtualisierte Betriebssystemumgebung MUSS als Betriebssystemasset erfasst und Gegenstand eines strengen Änderungsmanagements sein (siehe auch A_54412) [A_54469]. Zusätzlich müssen separate Prozesse für die Inbetriebnahme, den Betrieb und die Wartung von virtualisierten Betriebssystemumgebungen (Gästen) definiert und implementiert werden [A_54470].

Werden Gäste mit unterschiedlichen Sicherheitsanforderungen oberhalb des gleichen VMM betrieben, so stellt der Gast mit den geringeren Sicherheitsanforderungen immer eine zusätzliche Bedrohung für den Gast mit höheren Sicherheitsanforderungen dar. Gäste mit unterschiedlichen Sicherheitsanforderungen DÜRFEN daher NICHT oberhalb des gleichen VMM betrieben werden [A_54471]. Um die Bedrohung durch den VMM selbst zu minimieren, SOLL der VMM mit höheren Sicherheitsanforderungen wie die oberhalb des VMM betriebenen Gäste konfiguriert werden [A_54472]. Der VMM MUSS mindestens mit den gleichen Sicherheitsanforderungen wie die oberhalb des VMM betriebenen Gäste konfiguriert werden [A_54473]. Betriebssystemassets, die innerhalb des Sicherheitskonzeptes des Betreibers unabhängig voneinander betrachtet werden, DÜRFEN NICHT oberhalb des gleichen VMM betrieben werden [A_54474]. Die Verfügbarkeit von Gästen auf einem VMM MUSS innerhalb der Risikobetrachtung des Betreibers immer mit dem VMM gemeinsam berücksichtigt werden, da die Gäste jeweils vom VMM abhängig sind und durch die gemeinsame Nutzung des VMM auch zueinander eine Abhängigkeit besteht [A_54475].

Die Wahrscheinlichkeit von Sicherheitslücken innerhalb einer Virtualisierungstechnologie steigt mit deren Komplexität. Ein konzeptionell einfacher VMM kann die Sicherheit besser gewähren als ein komplexer VMM. Beispielsweise wird (informativ) zwischen Typ-I-VMM und Hosted- und Domain-Architektur unterschieden, wobei die Typ-I-VMM durch ihre Nähe zur Hardware eine geringere Komplexität aufweist. Ebenso wird (informativ)

zwischen CPU-unterstützter Virtualisierung (geringe Komplexität), Paravirtualisierung, Trap & Emulate und Binary Translation (sehr hohe Komplexität) unterschieden, wobei der CPU-unterstützten Virtualisierung der Vorzug zu geben ist, während die Binary Translation wenn möglich vermieden werden soll. Die hier informativ genannten Beispiele erheben keinen Anspruch auf Vollständigkeit und sind nur zum besseren Verständnis der Definition der Komplexität einer VMM herangezogen worden.

Das Sicherheitskonzept des Betreibers MUSS darlegen, welche Risiken durch die Wahl einer bestimmten Virtualisierungstechnologie auftreten und durch welche zusätzlichen Sicherheitsmaßnahmen diesen begegnet wird [A_54476]. Der Betreiber SOLL die Virtualisierungstechnologie mit der geringsten Komplexität wählen [A_54477].

Virtualisierungstechnologie erstreckt sich nicht nur über einzelne Gast-Systeme, sondern kann auch Netzwerkstrukturen beinhalten. Der Grundsatz der angestrebten geringen Komplexität (z. B. weist ein Switch eine geringere Komplexität als ein Router auf) gilt daher auch für virtualisierte Netzwerke. Hierbei ist jedoch zu beachten, dass ein virtueller Hub keinerlei Schutz gegen Abhören bietet, so dass bei virtualisierten Netzwerkkomponenten durch die gering zu haltende Komplexität nicht nur eine obere Grenze definiert wird, sondern durch die Auswahl zu einfacher Komponenten ebenfalls das Sicherheitsniveau gesenkt werden kann.

Wird innerhalb des VMM eine Virtualisierung des Netzwerkes durchgeführt, so DÜRFEN komplexe Netzwerkstrukturen NICHT virtualisiert werden [A_54478]. Das Abhören des Netzwerkverkehrs der Gäste untereinander MUSS im VMM verhindern werden [A_54479]. Netzwerkkomponenten mit Sicherheitsfunktionen DÜRFEN NICHT virtualisiert werden [A_54480].

Obwohl durch den Einsatz von Virtualisierungstechnologie eine bessere Ausnutzung der zur Verfügung stehenden Ressourcen angestrebt wird, wird durch ein Überbuchen der physikalisch verfügbaren Ressourcen oder eine komplexe Verwaltung der Ressourcen auch eine zusätzliche Bedrohung der Verfügbarkeit erzeugt.

Der VMM DARF allen Gästen zusammen NICHT mehr Ressourcen zuweisen als physikalisch vorhanden sind [A_54481]. Um eine komplexe Ressourcen-Verwaltung zu vermeiden DARF die Ressourcenzuweisung im VMM NICHT dynamisch erfolgen [A_54482].

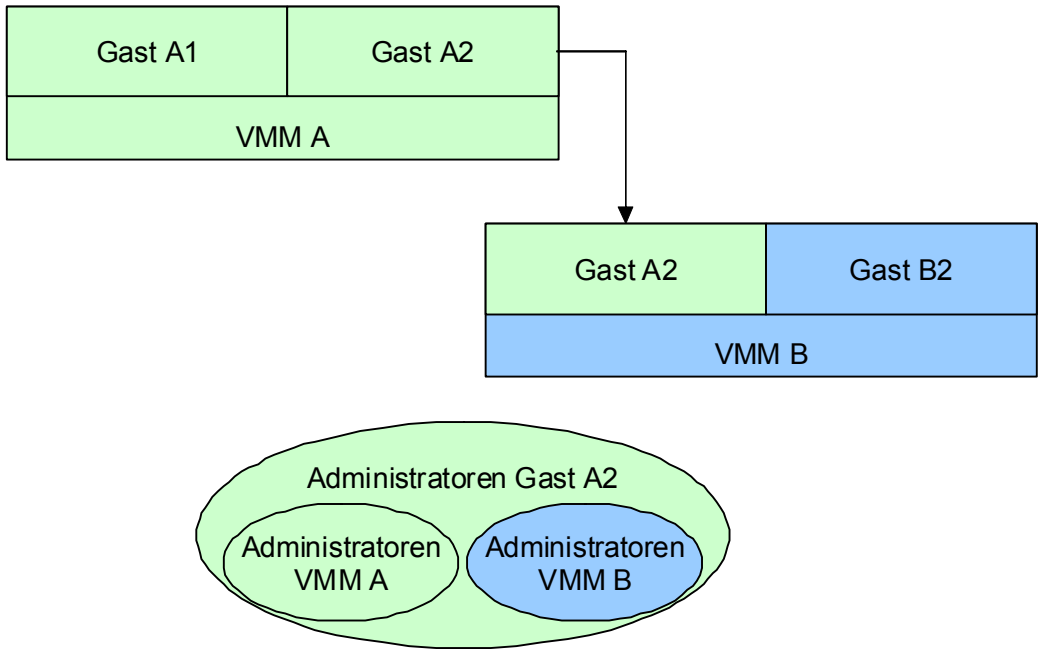

Abbildung AnhG-3.2.4.3: Schnittmengen der Personengruppen privilegierter Benutzer bei einem Gast-Umzug

Der privilegierte Zugang zu einem VMM stellt immer einen privilegierten Zugang zu jedem Gast, der oberhalb des VMM betrieben wird, dar. Selbst wenn ein direkter administrativer Zugriff auf den Gast nicht möglich ist, so kann die Verfügbarkeit des Gastes durch den privilegierten Zugang zum VMM beeinflusst werden. Im Sicherheitskonzept des Betreibers MÜSSEN Administratoren eines VMM daher zur gleichen Personengruppe gehören, wie die Administratoren jedes Gastes, der oberhalb des VMM betrieben wird [A_54483]. Ebenso DÜRFEN Gäste NICHT zu Systemen relokalisiert werden, deren Administratoren nicht der Personengruppe der Administratoren des Gastes angehören [A_54484].

In Abbildung AnhG-3.2.4.3: Schnittmengen der Personengruppen privilegierter Benutzer bei einem Gast-Umzug wird (informativ) ein solcher Umzug erläutert: der Gast A2 wird vom VMM A auf den VMM B relokalisiert. Vor dem Umzug ist der Administrator der VMM A bereits Teil des Personenkreises der Administratoren von Gast A2. Ebenso muss der Administrator der VMM B Teil des Personenkreises der Administratoren des Gastes A2 sein (oder diesem hinzugefügt werden). Der Administrator der VMM A ist nicht notwendigerweise der Administrator der VMM B, jedoch müssen beide Administratoren für den Gast A2 privilegiert sein.

G3.2.8 – Zusammenfassung der Sicherheitsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54468		S		Sämtliche für reale Betriebssystemumgebungen definierten und implementierten Schutzmaßnahmen und Sicherheitsprozesse (oder nachweisliche äquivalente Maßnahmen bzw. Prozesse) MÜSSEN auch auf virtualisierte Betriebssystemumgebungen angewendet werden.		Anhang G 3.2
A_54469		S		Jede virtualisierte Betriebssystemumgebung MUSS als Betriebssystemasset erfasst und Gegenstand eines strengen Änderungsmanagements sein.		Anhang G 3.2
A_54470		S		Der Betreiber MUSS im Änderungsmanagement separate Prozesse für die Inbetriebnahme, den Betrieb und die Wartung von virtualisierten Betriebssystemumgebungen (Gästen) definieren und implementieren.		Anhang G 3.2
A_54471		S		In einer virtualisierten Betriebssystemumgebung DÜRFEN Gäste mit unterschiedlichen Sicherheitsanforderungen NICHT oberhalb des gleichen VMM betrieben werden.		Anhang G 3.2
A_54472		S		Um die Bedrohung durch den VMM selbst zu minimieren, SOLL in einer virtualisierten Betriebssystemumgebung der VMM mit höheren Sicherheitsanforderungen als die oberhalb des VMM betriebenen Gäste konfiguriert werden.		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54473		S		In einer virtualisierten Betriebssystemumgebung MUSS der VMM mindestens mit den gleichen oder höheren Sicherheitsanforderungen wie die oberhalb des VMM betriebenen Gäste konfiguriert werden.		Anhang G 3.2
A_54474		S		Betriebssystemassets, die innerhalb des Sicherheitskonzeptes des Betreibers unabhängig voneinander betrachtet werden, DÜRFEN in einer virtualisierten Betriebssystemumgebung NICHT oberhalb des gleichen VMM betrieben werden.		Anhang G 3.2
A_54475		S		In einer virtualisierten Betriebssystemumgebung MUSS die Verfügbarkeit von Gästen auf einem VMM innerhalb der Risikobetrachtung des Betreibers immer gemeinsam berücksichtigt werden, da die Gäste jeweils vom VMM abhängig sind und durch die gemeinsame Nutzung des VMM auch zueinander eine Abhängigkeit besteht.		Anhang G 3.2
A_54476		S		Das Sicherheitskonzept des Betreibers MUSS darlegen, welche Risiken durch die Wahl einer bestimmten Virtualisierungstechnologie auftreten und durch welche zusätzlichen Sicherheitsmaßnahmen diesen begegnet wird.		Anhang G 3.2
A_54477		S		Der Betreiber SOLL die Virtualisierungstechnologie mit der geringsten Komplexität wählen.		Anhang G 3.2
A_54478		S		Wird innerhalb des VMM eine Virtualisierung des Netzwerkes durchgeführt, so DÜRFEN komplexe Netzwerkstrukturen NICHT virtualisiert werden.		Anhang G 3.2

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54479		S		In einer virtualisierten Betriebssystemumgebung MUSS das Abhören des Netzwerkverkehrs der Gäste untereinander im VMM verhindern werden.		Anhang G 3.2
A_54480		S		Netzwerkkomponenten mit Sicherheitsfunktionen DÜRFEN NICHT virtualisiert werden.		Anhang G 3.2
A_54481		S		In einer virtualisierten Betriebssystemumgebung DARF der VMM allen Gästen zusammen NICHT mehr Ressourcen zuweisen als physikalisch vorhanden sind.		Anhang G 3.2
A_54482		S		Um eine komplexe Ressourcen-Verwaltung zu vermeiden, DARF in einer virtualisierten Betriebssystemumgebung die Ressourcenzuweisung im VMM NICHT dynamisch erfolgen.		Anhang G 3.2
A_54483		S		Im Sicherheitskonzept des Betreibers MÜSSEN Administratoren eines VMM zur gleichen Personengruppe gehören wie die Administratoren jedes Gastes, der oberhalb des VMM betrieben wird.		Anhang G 3.2
A_54484		S		Bei Einsatz von virtualisierten Betriebssystemumgebung DÜRFEN Gäste NICHT zu Systemen relokalisiert werden, deren Administratoren nicht der Personengruppe der Administratoren des Gastes angehören.		Anhang G 3.2