Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.7 Systemmanagement

1. Beschreibung

1.1. Einleitung

Ein zuverlässiges Systemmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner vernetzter Systeme. Dazu ist es erforderlich, dass ein Systemmanagement alle relevanten Systeme umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Systemmanagement-Kommunikation und -infrastruktur zu schützen.

Das Systemmanagement umfasst viele wichtige Funktionen wie z. B. die Systemüberwachung, die Konfiguration der Systeme, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das auch als gemeinsame Plattform für IT-Systeme und Netzkomponenten angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Systemmanagement-Komponenten realisiert werden.

Die Systemmanagement-Lösung besteht aus verschiedenen Systemmanagement-Komponenten, zum Beispiel Agenten, die auf einer zugrundeliegenden Systemmanagement-Infrastruktur betrieben werden. Diese Lösung wird genutzt, um die eingebundenen und zu verwaltenden Systeme über die entsprechenden Schnittstellen des Informationsverbundes zu steuern. Die Kombination aus der Lösung, der zugrundeliegenden Infrastruktur, den zu verwaltenden Systemen und dem Betrieb bildet die Gesamtheit des Systemmanagements.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil des Systemmanagements zu etablieren. Der Baustein beschreibt zum einen, wie das Systemmanagement aufgebaut und abgesichert werden kann, und zum anderen, wie die zugehörige Kommunikation geschützt werden kann.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.7 *Systemmanagement* ist auf die Systemmanagement-Lösung anzuwenden, die im Informationsverbund eingesetzt wird.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt z. B.

- die notwendigen Systemmanagement-Komponenten,
- die konzeptionellen Aufgaben zum Systemmanagement,
- Protokollierung unter dem Gesichtspunkt des Systemmanagements sowie
- die Aktualisierung der Systemmanagement-Lösung.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Anforderungen zum Netzmanagement (siehe NET.1.2 *Netzmanagement)*
- Details bezüglich der Absicherung der zugrundeliegenden Infrastruktur und von zu verwaltenden IT-Systemen, insbesondere deren Management-Schnittstellen (siehe SYS.2 *IT-Systeme)*
- Protokollierungs- und Archivierungskonzepte (siehe OPS.1.1.5 *Protokollierung*, OPS.1.2.2 *Archivierung*)
- Aktualisierung z. B. durch Zusatzsoftware, sogenannte Agenten (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- Zugriffe von Benutzenden auf die Systemmanagement-Lösung (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*, sowie OPS.1.2.5 *Fernwartung* und OPS.1.1.2 *Ordnungsgemäße IT-Administration*).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.7 *Systemmanagement* von besonderer Bedeutung.

2.1. Unberechtigter Zugriff auf die Systemmanagement-Lösung

Das Systemmanagement ist aufgrund seiner zentralen Stellung und aufgrund der notwendigen Zugriffsrechte auf alle zu verwaltenden Systeme ein vorrangiges Ziel für Angriffe.

Wenn es Angreifenden gelingt auf Systemmanagement-Lösungen zuzugreifen, z. B. durch ungepatchte Sicherheitslücken, dann können diese alle vom Systemmanagement verwalteten Systeme kontrollieren und neu konfigurieren. So können sie z. B. auf schützenswerte Informationen zugreifen oder auch Dienste oder verwaltete Systeme stören. Beispielsweise könnte ein Unternehmen zentral Konfigurationsserver für eine Systemmanagementlösung bereitstellen. Über eine ungepatchte Schwachstelle werden in diesem Beispiel die Konfigurationsdateien so verändert, dass die verwalteten Systeme eine Ransomware installieren. In Folge werden in diesem Beispiel alle Systeme, die von dieser Systemmanagementlösung verwaltet werden, verschlüsselt.

2.2. Fehler in Automatisierungsfunktionen für das Systemmanagement

Alle Schutzziele des zu verwaltenden Informationssysteme können durch fehlerhaft automatisierte Abläufe beeinträchtigt sein.

Durch Fehler in einer oder mehreren Automatisierungsfunktionen wie z. B. Skripte, können die zu verwaltenden Systeme funktionsunfähig oder kompromittiert werden. Wegen der automatisierten Abläufe kann schnell eine große Anzahl von IT-Systemen kompromittiert werden. Auch besonders kritische IT-Systeme können auf diesem Weg schnell kompromittiert werden.

2.3. Unberechtigte Eingriffe in die Systemmanagement-Kommunikation

Versehentliche Eingriffe in oder gezielte Angriffe auf die Kommunikation des Systemmanagements können die Integrität der verwalteten IT-Systeme verletzen und die Verfügbarkeit von Diensten oder IT-Systemen einschränken.

Wird die Systemmanagement-Kommunikation abgehört und manipuliert, dann können auf diesem Weg aktive Systeme kontrolliert werden. Außerdem können die von und zu den Systemen übertragenen Daten mitgeschnitten und eingesehen werden.

2.4. Unzureichende Zeitsynchronisation der Systemmanagement-Komponenten

Fehler in der Zeitsynchronisation können Probleme und Ereignisse verdecken, sodass z. B. die Erkennung von Sicherheitsvorfällen und Datenabflüssen erschwert wird.

Wenn die Systemzeit der Systemmanagement-Komponenten unzureichend synchronisiert wird, dann können (beispielsweise) Protokolle, die unter anderem Zeitstempel zur Evaluierung der Kommunikationsgültigkeit verwenden, durch unterschiedliche Systemzeiten auf den Systemmanagement-Komponenten und den zu verwaltenden Systemen gestört werden.

Zusätzlich können die Protokollierungsdaten zum Systemmanagement unter Umständen eventuell nicht miteinander korreliert werden. Auch kann die Korrelation eventuell zu fehlerhaften Aussagen führen, wenn Zeitstempel aufgrund fehlerhafter Synchronisation nur scheinbar übereinstimmen oder abweichen.

2.5. Inkompatibilität zwischen den zu verwaltenden Systemen und der Systemmanagement-Lösung

Eine nur unvollständig kompatible Systemmanagement-Lösung kann Fehlfunktionen der zu verwaltenden IT-Systeme auslösen und deren Verfügbarkeit einschränken.

Falls die Systemmanagement-Lösung die zu verwaltenden IT-Systeme nicht vollständig unterstützt, können bestimmte Aktionen nicht wie geplant durchgeführt werden. Diese Gefährdung kann auch bei einer Aktualisierung der Systeme auftreten, bei der die Management-Schnittstellen verändert werden.

2.6. Verbindungsverlust zwischen Anwendenden und Systemmanagement-Lösung

Verbindungsabbrüche können die Verfügbarkeit der Systemmanagement-Lösung einschränken.

Wenn die Verbindung zwischen den Administrierenden und der Systemmanagement-Lösung gestört wird, können IT-Systeme ausfallen. Außerdem können eine Fehlerbehebung und die Verwaltung von IT-Systemen erschwert werden.

Wenn eine Verbindung abbricht oder gestört wird, dann können kostenintensive sicherheitsrelevante sowie zeitkritische Arbeiten nicht fristgerecht durchgeführt werden, beispielsweise können Sicherheitsupdates nicht mehr eingespielt werden oder auf Sicherheitsvorfälle nicht angemessen reagiert werden.

2.7. Verbindungsverlust zwischen Systemmanagement-Lösung und zu verwaltenden Systemen

Verbindungsabbrüche zu den zu verwaltenden Systemen können insbesondere die Verfügbarkeit oder Integrität von Diensten im Informationsverbund beeinträchtigen.

Der Umfang und die Konstellation eines solchen Verbindungsverlusts entscheiden darüber, ob Dienste beeinträchtigt werden und welche Schäden entstehen können. Die resultierenden Fehlerbilder sind unter Umständen schwer zu analysieren und die auftretenden Fehler schwer zu beheben.

2.8. Unzureichende Abstimmung zwischen Systemmanagement und Netzmanagement

Nicht abgestimmte Aktionen im Netzmanagement können sich negativ auf das Systemmanagement auswirken. Dadurch können Inkonsistenzen in der Konfiguration zwischen IT-Systemen und verbindenden Netzen entstehen. So können z. B. Verbindungsverluste im Netz eine große Anzahl von Folgeereignissen im Bereich Systemmanagement auslösen. Diese Ereignisse können bis zu Fehlkonfigurationen reichen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.7 *Systemmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.7.A1 Anforderungsspezifikation für das Systemmanagement (B)

Anforderungen an die Systemmanagement-Infrastruktur und -Prozesse MÜSSEN spezifiziert werden. Dabei MÜSSEN alle wesentlichen Elemente für das Systemmanagement berücksichtigt werden. Auch MÜSSEN die Sicherheitsaspekte für das Systemmanagement von Beginn an beachtet werden.

Zudem MÜSSEN die Schnittstellen der zu verwaltenden IT-Systeme dokumentiert werden, z. B. um die Kompatibilität von Systemmanagement-Lösung und zu verwaltendem System zu gewährleisten.

OPS.1.1.7.A2 Planung des Systemmanagements (B)

Die Systemmanagement-Lösung und die zugrundeliegende Infrastruktur MÜSSEN geeignet geplant werden. Die Planung MUSS mindestens die folgenden Inhalte umfassen:

- eine detaillierte Anforderungsanalyse,
- ein aussagekräftiges Grobkonzept,
- einen umfassenden Umsetzungsplan sowie
- Meilensteine für Qualitätssicherung und Abnahme.

Dabei MÜSSEN alle in der Anforderungsspezifikation genannten Punkte sowie das Rollen- und Berechtigungskonzept berücksichtigt werden. Es MÜSSEN mindestens die folgenden Themen berücksichtigt werden:

- Trennung in geeignete Bereiche für das Systemmanagement,
- Zugriffsmöglichkeiten auf und durch das Systemmanagement,
- Berechtigungen des Systemmanagements auf den zu verwaltenden Systemen,
- Netzverbindungen für den Zugriff auf und durch das Systemmanagement,
- Protokolle für den Zugriff von Benutzenden auf die Systemmanagement-Lösung,
- Protokolle für die Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen,
- Anforderungen an Systemmanagement-Werkzeuge,
- Schnittstellen, um erfasste Ereignis- oder Alarmmeldungen weiterzuleiten,
- Protokollierung, inklusive erforderlicher Schnittstellen zu einer zentralen Protokollierungslösung,
- Unterstützung durch das herstellende bzw. entwickelnde Unternehmen über den geplanten Einsatzzeitraum,
- Möglichkeiten zum Einspielen von Patches für die Systemmanagement-Lösung sowie für die zu verwaltenden Systeme,
- Reporting und Schnittstellen zu übergreifenden Lösungen sowie
- korrespondierende Anforderungen an die zu verwaltenden Systeme.

OPS.1.1.7.A3 Zeitsynchronisation für das Systemmanagement (B)

Alle Komponenten der Systemmanagement-Lösung, inklusive der zu verwaltenden Systeme, MÜSSEN eine synchrone Uhrzeit nutzen. Die Systemzeit MUSS für jedes zu verwaltende System und für die Systemmanagement-Lösung über geeignete Protokolle synchronisiert werden.

OPS.1.1.7.A4 Absicherung der Systemmanagement-Kommunikation (B)

Sobald die Systemmanagement-Lösung und die zu verwaltenden Systeme über die produktive Infrastruktur kommunizieren, MÜSSEN dafür sichere Protokolle verwendet werden. Falls keine sicheren Protokolle verwendet werden können, dann MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe NET.1.1 *Netzarchitektur und -design*). Ist auch dies nicht möglich, dann MÜSSEN ergänzende Sicherheitsmechanismen auf anderer Ebene eingesetzt werden, z. B. Tunnelmechanismen über verschlüsseltes VPN oder vergleichbare Lösungen.

OPS.1.1.7.A5 Gegenseitige Authentisierung von Systemmanagement-Lösung und zu verwaltenden Systemen (B)

Die Authentisierung zwischen Systemmanagement-Lösung und zu verwaltenden Systemen MUSS in beide Richtungen erfolgen. Die Authentisierung MUSS in das übergreifende Authentisierungskonzept eingebunden sein. Die Authentisierung MUSS mittels sicherer Protokolle erfolgen.

OPS.1.1.7.A6 Absicherung des Zugriffs auf die Systemmanagement-Lösung (B)

Der Zugriff von Benutzenden auf die Systemmanagement-Lösung MUSS abgesichert werden durch

- eine sichere und angemessene Authentisierung und Autorisierung der Benutzenden sowie
- eine sichere Verschlüsselung der übertragenen Daten.

Eine angemessene Authentisierungsmethode MUSS ausgewählt werden. Der Auswahlprozess MUSS dokumentiert werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel MUSS regelmäßig überprüft und bei Bedarf angepasst werden.

Die Systemmanagement-Lösung MUSS über eine Autorisierungskomponente sicherstellen, dass Benutzende ausschließlich solche Aktionen durchführen können, zu denen sie berechtigt sind.

3.2. Standard-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.7.A7 Festlegung einer Sicherheitsrichtlinie für das Systemmanagement (S)

Für das Systemmanagement SOLLTE eine Sicherheitsrichtlinie erstellt und nachhaltig gepflegt werden. Die Richtlinie SOLLTE allen Personen, die am Systemmanagement beteiligt sind, bekannt sein. Die Sicherheitsrichtlinie SOLLTE zudem grundlegend für die Arbeit dieser Personen sein. Es SOLLTE regelmäßig und nachvollziehbar überprüft werden, dass die in der Richtlinie geforderten Inhalte umgesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

Die Sicherheitsrichtlinie SOLLTE mindestens das Folgende festlegen:

- die Bereiche des Systemmanagements, die über zentrale Management-Werkzeuge und -Dienste realisiert werden,
- die Aufgaben im Systemmanagement, die automatisiert realisiert werden sollen,
- das Konfigurationsmanagement für die Daten, die von der Systemmanagement-Lösung verwaltet werden, z. B. Versionierung von Konfigurationen,
- Vorgaben für die Netztrennung,
- Vorgaben für die Zugriffskontrolle,
- Vorgaben für die Protokollierung,
- Vorgaben für die Qualitätssicherung beim Einsatz von Automatisierungsfunktionen, z. B. Skripte,
- Vorgaben für den Schutz der Kommunikation,
- die operativen Grundregeln des Systemmanagements sowie
- Vorgaben für die Abstimmung mit dem Netzmanagement, z. B. Vergabe von IP-Adressen oder DNS-Namen.

OPS.1.1.7.A8 Erstellung eines Systemmanagement-Konzepts (S)

Ausgehend von der Sicherheitsrichtlinie für das Systemmanagement SOLLTE ein Systemmanagement-Konzept erstellt und kontinuierlich gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das Systemmanagement,
- Absicherung des Zugangs und der Kommunikation,

- Absicherung auf Ebene des Netzes, insbesondere Zuordnung von Systemmanagement-Komponenten zu Sicherheitszonen,
- Umfang des Monitorings und der Alarmierung für jedes zu verwaltende System,
- Protokollierung,
- Automatisierung, insbesondere die zentrale Verteilung von Konfigurationsdateien auf die zu verwaltenden Systeme,
- Vorgaben an Entwicklung und Test von Automatisierungsfunktionen,
- Meldeketten bei Störungen und Sicherheitsvorfällen,
- Bereitstellung von Systemmanagement-Informationen für andere Betriebsbereiche,
- Einbindung des Systemmanagements in die Notfallplanung, sowie
- benötigten Netzübertragungskapazitäten der Systemmanagement-Lösung.

OPS.1.1.7.A9 Fein- und Umsetzungsplanung für das Systemmanagement (S)

Eine Fein- und Umsetzungsplanung für die Systemmanagement-Lösung SOLLTE erstellt werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und im Systemmanagement-Konzept adressierten Punkte berücksichtigt werden.

OPS.1.1.7.A10 Konzept für den sicheren Betrieb der Systemmanagement-Lösung (S)

Ausgehend von den Sicherheitsrichtlinien und dem Systemmanagement-Konzept SOLLTE ein Konzept für den sicheren Betrieb der Systemmanagement-Lösung und der zugrundeliegenden Infrastruktur erstellt werden.

Auch SOLLTE geprüft werden, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

OPS.1.1.7.A11 Regelmäßiger Soll-Ist-Vergleich im Rahmen des Systemmanagements (S)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, inwieweit die von der Systemmanagement-Lösung verwalteten Daten, Konfigurationen und Skripte dem Sollzustand entsprechen. Mindestens folgende Aspekte SOLLTEN im Soll-Ist-Vergleich geprüft werden:

- die Konfiguration der Systemmanagement-Lösung,
- die Konfiguration der zu verwaltenden Systeme sowie
- die eingesetzten Automatisierungsfunktionen oder Skripte.

Dabei SOLLTE geprüft werden, ob die genannten Aspekte noch die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllen. Weiter SOLLTE verglichen werden, ob die Softwareversion der Systemmanagement-Lösung aktuell ist.

OPS.1.1.7.A12 Auslösung von Aktionen durch die zentralen Komponenten der Systemmanagement-Lösung (S)

Aktionen, die durch das Systemmanagement auf den verwalteten Systemen ausgeführt werden, SOLLTEN ausschließlich von der Systemmanagement-Lösung ausgelöst werden. Dafür SOLLTEN nur diejenigen Management-Funktionen auf der Systemmanagement-Lösung und den zu verwaltenden Systemen aktiviert werden, die tatsächlich benötigt werden.

OPS.1.1.7.A13 Verpflichtung zur Nutzung der vorgesehenen Schnittstellen für das Systemmanagement (S)

Management-Zugriffe auf zu verwaltende Systeme SOLLTEN ausschließlich über die dafür vorgesehenen Schnittstellen der Systemmanagement-Lösung erfolgen. Falls ein direkter Zugriff auf zu verwaltende Systeme notwendig ist, z. B. nach einem Ausfall eines zu verwaltenden Systems, SOLLTEN sowohl der direkte Zugriff als auch alle in diesem Rahmen vorgenommenen Änderungen dokumentiert und im notwendigen Umfang in die Systemmanagement-Lösung eingepflegt werden.

OPS.1.1.7.A14 Zentrale Konfigurationsverwaltung für zu verwaltende Systeme (S)

Software und Konfigurationsdaten für die zu verwaltenden Systeme SOLLTEN konsequent in einem Konfigurationsmanagement verwaltet werden, das eine Versionierung und Änderungsverfolgung ermöglicht. Die zugehörige Dokumentation zur Konfigurationsverwaltung SOLLTE vollständig und immer aktuell sein. Die benötigten Dokumentationen SOLLTEN an zentraler Stelle sicher verfügbar sein sowie in die Datensicherung eingebunden werden. Die zentrale Konfigurationsverwaltung SOLLTE nachhaltig gepflegt und regelmäßig auditiert werden.

Sämtliche Schnittstellen zwischen Systemmanagement-Lösung und anderen Anwendungen und Diensten SOLLTEN dokumentiert und vollständig in einem Konfigurationsmanagement verwaltet werden. Zwischen relevanten Betriebsbereichen SOLLTEN funktionale Änderungen an den Schnittstellen frühzeitig abgestimmt und dokumentiert werden.

Die Konfigurationsdaten für die zu verwaltenden Systeme SOLLTEN automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert werden können.

OPS.1.1.7.A15 Statusüberwachung, Protokollierung und Alarmierung bei relevanten Ereignissen im Systemmanagement-Lösung und den zu verwaltenden Systemen (S)

Die grundlegenden Performance- und Verfügbarkeitsparameter der Systemmanagement-Lösung und der zu verwaltenden Systeme SOLLTEN kontinuierlich überwacht werden. Dafür SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining). Werden definierte Schwellwerte überschritten, SOLLTE das zuständige Personal automatisch benachrichtigt werden.

Zur besseren Fehleranalyse SOLLTEN Informationen aus der Statusüberwachung anderer Bereiche, z. B. aus einem eigenen Bereich „Netze“, ebenfalls betrachtet werden, um die genaue Ursache für eine Störung zu finden.

Wichtige Ereignisse auf zu verwaltenden Systemen und auf der Systemmanagement-Lösung SOLLTEN automatisch an eine zentrale Protokollierungsinfrastruktur übermittelt und dort protokolliert werden (siehe OPS.1.1.5 *Protokollierung*).

Wichtige Ereignisse SOLLTEN mindestens für folgende Aspekte definiert werden:

- Ausfall sowie Nichterreichbarkeit von zu verwaltenden Systemen,
- Ausfall sowie Nichterreichbarkeit von Systemmanagement-Komponenten,
- Hardware-Fehlfunktionen,
- Anmeldeversuche an der Systemmanagement-Lösung,
- Anmeldeversuche an zu verwaltenden Systemen,
- kritische Zustände oder Überlastung der Systemmanagement-Lösung sowie
- kritische Zustände oder Überlastung von zu verwaltenden Systemen.

Ereignismeldungen sowie Protokollierungs-Daten SOLLTEN an ein zentrales Logging-System übermittelt werden. Alarmmeldungen SOLLTEN sofort, wenn sie auftreten, übermittelt werden.

OPS.1.1.7.A16 Einbindung des Systemmanagements in die Notfallplanung (S)

Die Systemmanagement-Lösung SOLLTE in die Notfallplanung der Institution eingebunden werden. Dazu SOLLTEN sowohl die Systemmanagement-Lösung als auch die Konfigurationen der zu verwaltenden Systeme gesichert und in die Wiederanlaufpläne integriert sein.

OPS.1.1.7.A17 Kontrolle der Systemmanagement-Kommunikation (S)

Die Kommunikation zwischen den Benutzenden und der Systemmanagement-Lösung sowie zwischen der Systemmanagement-Lösung und den zu verwaltenden IT-Systemen SOLLTE über geeignete Filtertechniken auf unbedingt notwendige Verbindungen eingeschränkt werden.

OPS.1.1.7.A18 Überprüfung des Systemzustands (S)

Die Konsistenz zwischen realem Systemzustand und dem von der Systemmanagement-Lösung angenommenen Zustand SOLLTE regelmäßig geprüft werden. Werden Abweichungen festgestellt, SOLLTE der in der Systemmanagement-Lösung vorgesehene Zustand wiederhergestellt werden.

OPS.1.1.7.A19 Absicherung der Systemmanagement-Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen (S)

Die Systemmanagement-Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen SOLLTE grundsätzlich verschlüsselt sein. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.7.A20 Hochverfügbare Realisierung der Systemmanagement-Lösung (H)

Eine zentrale Systemmanagement-Lösung SOLLTE hochverfügbar betrieben werden. Dazu SOLLTEN die für die Systemmanagement-Lösung eingesetzten Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt sein.

OPS.1.1.7.A21 Physische Trennung der zentralen Systemmanagementnetze (H)

Das Managementnetz für das Systemmanagement SOLLTE physisch von den funktionalen, insbesondere produktiven, Netzen getrennt werden.

OPS.1.1.7.A22 Einbindung des Systemmanagements in automatisierte Detektionssysteme (H)

Die Protokollierung von sicherheitsrelevanten Ereignissen des Systemmanagements SOLLTE in ein Security Information and Event Management (SIEM) eingebunden werden. Dabei SOLLTE nachvollziehbar festgelegt werden, welche Ereignisse an das SIEM weitergeleitet werden.

Im Anforderungskatalog zur Auswahl einer Systemmanagement-Lösung SOLLTEN die erforderlichen Schnittstellen und Übergabeformate spezifiziert werden.

Eine Systemmanagement-Lösung SOLLTE mit einem System zur Erkennung sicherheitsrelevanter Schwachstellen automatisiert überwacht werden.

OPS.1.1.7.A23 Standort-übergreifende Zeitsynchronisation für das Systemmanagement (H)

Die Zeitsynchronisation SOLLTE sowohl für die Systemmanagement-Lösung als auch für die zu verwaltenden Systeme über alle Standorte der Institution sichergestellt werden. Dafür SOLLTE eine gemeinsame Referenzzeit benutzt werden.

OPS.1.1.7.A24 Automatisierte Überprüfung von sicherheitsrelevanten Konfigurationen durch geeignete Detektionssysteme (H)

Sicherheitsrelevante Konfigurationen der Systemmanagement-Lösung und der zu verwaltenden Systeme SOLLTEN durch geeignete Detektionssysteme regelmäßig auf Abweichungen vom Sollzustand sowie auf potenzielle Schwachstellen überprüft werden.

OPS.1.1.7.A25 Protokollierung und Reglementierung von Systemmanagement-Sitzungen (H)

Die Sitzungsinhalte, insbesondere die Aktivitäten von Benutzenden auf der Systemmanagement-Lösung sowie sämtliche direkte Zugriffe auf zu verwaltende Systeme, SOLLTEN kontinuierlich durch eine technische Lösung protokolliert und reglementiert werden. Dabei SOLLTEN die Aktivitäten auf Befehlsebene, d. h. manuelle und automatisierte Befehle, kontrolliert und gegebenenfalls unterbunden werden.

Während der Überwachung SOLLTE nicht nur bei konkreten Regelverstößen, sondern auch bei Anomalien im Benutzendenverhalten eine Alarmierung erfolgen.

OPS.1.1.7.A26 Entkopplung von Zugriffen auf die Systemmanagement-Lösung (H)

Jeder administrative Zugriff auf die Systemmanagement-Lösung SOLLTE durch die Nutzung von Sprungservern abgesichert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein OPS.1.1.7 *Systemmanagement* sind keine weiterführenden Informationen vorhanden.