Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.7 IBM Z

1. Beschreibung

1.1. Einleitung

Systeme vom Typ „IBM Z“ gehören zu den Server-Systemen, die allgemein als Großrechner („Mainframes“) bezeichnet werden. Großrechner haben sich von klassischen Einzelsystemen mit Stapelverarbeitung hin zu modernen Client-Server-Systemen entwickelt. Die Z-Architektur ist der Nachfolger der 1964 eingeführten S/360-Architektur und wird bei heutigen Großrechner-Installationen häufig eingesetzt.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Z-Systemen verarbeitet, angeboten oder darüber übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.7 *IBM Z* ist auf jeden Server anzuwenden, der auf der Z-Architektur von IBM basiert.

Der Baustein SYS.1.1 *Allgemeiner Server* bildet die Grundlage für die Absicherung von Servern. Für Z-Systeme müssen sowohl die dort aufgeführten allgemeinen Anforderungen als auch die konkreten Anforderungen im vorliegenden Baustein erfüllt werden.

Für die Z-Hardware sind verschiedene Betriebssysteme verfügbar (z. B. z/OS, z/VM, KVM oder Linux on Z). Die Auswahl erfolgt in der Regel anhand der Parameter Rechnergröße und Einsatzzweck. Die Empfehlungen dieses Bausteins beschränken sich im Wesentlichen auf das Betriebssystem z/OS. Ausgewählte Sicherheitsaspekte von z/VM werden ebenfalls angesprochen. Für das Betriebssystem Linux on Z wird auf den Baustein SYS.1.3 *Server unter Linux und Unix* verwiesen.

Weitere für IBM Z besonders relevante Anforderungen finden sich im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* sowie in OPS.1.2.5 *Fernwartung*.

Ein wichtiger Bestandteil der Sicherheitskonzeption von Z-Systemen auf technischer Ebene ist das eingesetzte Sicherheitssystem, beispielsweise TopSecret, ACF2 (Access Control Facility) oder RACF (Resource Access Control Facility). Um die Darstellung zu vereinfachen, wird im Folgenden nur auf RACF eingegangen. Die Empfehlungen sind entsprechend anzupassen, wenn ein anderes Sicherheitssystem eingesetzt wird.

Die jeweils spezifischen Dienste, die vom Z-System angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Dienste müssen zusätzlich noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der IT-Grundschutz-Modellierung.

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 SYS.1.7 *IBM Z* von besonderer Bedeutung.

2.1. Unzureichende oder fehlerhafte Konfiguration der Hardware oder des z/OS-Betriebssystems

Die Konfiguration eines z/OS-Betriebssystems ist sehr komplex und erfordert an vielen Stellen den Eingriff durch Systemadministrierende. Durch falsche oder unzureichende Konfiguration können Schwachstellen entstehen, die zu entsprechenden Sicherheitsproblemen führen können. SuperVisor Calls (SVCs) sind beispielsweise Aufrufe zu speziellen z/OS-Dienstprogrammen, die im hoch autorisierten Kernel-Modus laufen. Unsichere SVC-Programme können unter Umständen benutzt werden, um z/OS-Sicherheitsmechanismen zu umgehen.

2.2. Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF

In einem z/OS-Betriebssystem ist für die Authentisierung von Benutzenden und deren Autorisierung auf Ressourcen ein spezielles Sicherheitssystem zuständig. Hierfür wird häufig RACF eingesetzt. Die Konfiguration von RACF im Auslieferungszustand entspricht in der Regel nicht den Sicherheitsanforderungen im jeweiligen Einsatzszenario. Die Ressourcen und z/OS-System-Kommandos werden beispielsweise über spezielle Klassen im RACF geschützt. Durch unzureichende Definitionen dieser Klassen ist es möglich, dass Benutzende Systembefehle absetzen können, die unter Umständen den stabilen Systembetrieb beeinträchtigen.

2.3. Fehlbedienung der z/OS-Systemfunktionen

Aufgrund der Komplexität eines z/OS-Betriebssystems und seiner Komponenten können Fehlbedienungen nicht vollständig ausgeschlossen werden. Je nach Art der Fehlbedienung können in der Folge einzelne Komponenten oder das gesamte System ausfallen. Verriegeln sich zum Beispiel Ressourcen gegenseitig (Contention), können bestimmte Funktionen so lange nicht verfügbar sein, bis die Verriegelung wieder gelöst wird. Oft sind eine Reihe von Systemabfragen (Displays) und viel Betriebserfahrung notwendig, um gegenseitige Verriegelungen mithilfe der richtigen z/OS-Kommandos wieder aufzulösen.

2.4. Manipulation der z/OS-Systemsteuerung

z/OS-Systeme lassen sich über vielfältige Schnittstellen beeinflussen, zum Beispiel über die Hardware Management Console, lokale sowie entfernte MCS-Konsolen, Automationsverfahren und Fernwartungszugänge. Wenn beispielsweise der physische oder der logische Zugang zu entfernten MCS-Konsolen unzureichend geschützt ist, können die z/OS-Systeme unter Umständen von dort aus unbefugt manipuliert werden.

2.5. Angriffe über TCP/IP auf z/OS-Systeme

Um ein z/OS-System über die Netzanbindung anzugreifen, sind häufig keine Spezialkenntnisse der Netzarchitektur oder von z/OS erforderlich. Durch die TCP/IP-Anbindung an (unter Umständen

öffentliche) Netze und die Unix System Services sind viele z/OS-Systeme über Standardprotokolle und Dienste, wie z. B. HTTP oder FTP, für interne bzw. externe Angriffe erreichbar. Bei externen Angriffen können unter Umständen über die TCP/IP-Anbindung an öffentliche Netze Denial-of-Service-Angriffe gegen die angebotenen Dienste durchgeführt oder übertragene Daten unbefugt gelesen oder manipuliert werden. Interne Angreifende können über die TCP/IP-Anbindung an interne Netze versuchen, ihre Berechtigungen zu erhöhen, indem sie etwa Kennung und Passwort von Benutzenden mit SPECIAL-Rechten ausspähen.

2.6. Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS

EBCDIC, ASCII und Unicode sind Zeichensätze, die festlegen, wie Buchstaben, Ziffern und andere Zeichen mithilfe von Bits dargestellt werden. z/OS-Systeme arbeiten mit EBCDIC-Code. Lediglich HFS- und zFS-Dateisysteme, die unter Unix System Services (USS) eingesetzt werden, lassen sowohl ASCII- als auch EBCDIC-Speicherung zu. Beim Datenaustausch zwischen z/OS-Systemen und IT-Systemen, die mit ASCII oder Unicode arbeiten (z. B. auch von USS nach z/OS), besteht die Gefahr, dass Informationen verfälscht werden, wenn fehlerhafte Übersetzungstabellen (Code Page Translation) eingesetzt werden. Besonders häufig betroffen ist dabei die Übersetzung von Sonderzeichen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.7 *IBM Z* 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	Vorgesetzte

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.

SYS.1.7.A1 Einsatz restriktiver z/OS-Kennungen (B)

Berechtigungen mit hoher Autorisierung DÜRFEN NUR an Benutzende vergeben werden, die diese Rechte für ihre Tätigkeiten benötigen. Insbesondere die RACF-Attribute SPECIAL, OPERATIONS, AUDITOR und die entsprechenden GROUP-Attribute sowie die User-ID 0 unter den Unix System Services (USS) MÜSSEN restriktiv gehandhabt werden. Die Vergabe und der Einsatz dieser Berechtigungen MÜSSEN nachvollziehbar sein. Die besondere Kennung IBMUSER DARF NUR bei der Neuinstallation zur Erzeugung von Kennungen mit Attribut SPECIAL benutzt werden. Diese Kennung MUSS danach dauerhaft gesperrt werden. Um zu vermeiden, dass Administrierende sich dauerhaft aussperren, MUSS ein Notfall-User-Verfahren eingerichtet werden.

SYS.1.7.A2 Absicherung sicherheitskritischer z/OS-Dienstprogramme (B)

Sicherheitskritische (Dienst-)Programme und Kommandos sowie deren Alias-Namen MÜSSEN mit Rechten auf entsprechende RACF-Profile so geschützt werden, dass sie nur von den dafür

vorgesehenen und autorisierten Personen benutzt werden können. Es MUSS sichergestellt sein, dass (Fremd-)Programme nicht unerlaubt installiert werden können. Außerdem DÜRFEN Programme NUR von gesicherten Quellen und über nachvollziehbare Methoden (z. B. SMP/E) installiert werden.

SYS.1.7.A3 Wartung von Z-Systemen (B)

Die Z-Hardware und -Firmware, das Betriebssystem sowie die verschiedenen Programme MÜSSEN regelmäßig und bei Bedarf gepflegt werden. Die hierfür notwendigen Wartungsaktivitäten MÜSSEN geplant und in das Änderungsmanagement (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*) integriert werden. Insbesondere DÜRFEN Updates durch das herstellende Unternehmen NUR unter Kontrolle der Betreibenden durchgeführt werden, lokal über SE (Support Elements) bzw. HMC (Hardware Management Console) oder remote über die RSF (Remote Support Facility).

SYS.1.7.A4 Schulung des z/OS-Bedienungspersonals (B) [Vorgesetzte]

Administrierende, Bedienende und Prüfende im z/OS-Bereich MÜSSEN entsprechend ihren Aufgaben ausgebildet sein. Insbesondere MÜSSEN RACF-Administrierende mit dem Sicherheitssystem selbst sowie gegebenenfalls mit den weiteren für sie relevanten Funktionen vertraut sein.

SYS.1.7.A5 Einsatz und Sicherung systemnaher z/OS-Terminals (B)

Systemnahe z/OS-Terminals MÜSSEN physisch gegen unbefugten Zutritt und logisch gegen unbefugten Zugang geschützt werden. Insbesondere die Support-Elemente sowie die HMC-, MCS-, SMCS-, Extended MCS- und Monitor-Konsolen MÜSSEN dabei berücksichtigt werden. Voreingestellte Passwörter MÜSSEN geändert werden. Zugänge über Webserver und andere Fernzugänge MÜSSEN durch Verschlüsselung geschützt werden. Nicht benötigte Webserver und Fernzugänge MÜSSEN deaktiviert werden, wenn sie nicht benötigt werden.

SYS.1.7.A6 Einsatz und Sicherung der Remote Support Facility (B)

Es MUSS entschieden werden, ob und gegebenenfalls wie RSF eingesetzt wird. Der Einsatz MUSS im Wartungsvertrag vorgesehen und mit dem Hardware-Support abgestimmt sein. Es MUSS sichergestellt werden, dass die RSF-Konfiguration nur von hierzu autorisierten Personen geändert werden kann. Wartungszugriffe für Firmware-Modifikationen durch das herstellende Unternehmen MÜSSEN von Betreibenden explizit freigegeben und nach Beendigung wieder deaktiviert werden. Die RSF-Kommunikation MUSS über Proxy-Server und zusätzlich über gesicherte Verbindungen (wie TLS) stattfinden.

SYS.1.7.A7 Restriktive Autorisierung unter z/OS (B)

Im Rahmen der Grundkonfiguration MÜSSEN die Autorisierungsmechanismen so konfiguriert werden, dass alle Personen (definierte User-IDs in Gruppen gemäß Rolle) nur die Zugriffsmöglichkeiten erhalten, die sie für ihre jeweiligen Tätigkeiten benötigen. Hierfür MÜSSEN insbesondere APF-Autorisierungen (Authorized Program Facility), SVCs (SuperVisor Calls), Ressourcen des z/OS-Betriebssystems, IPL-Parameter, Parmlib-Definitionen, Started Tasks und JES2/3-Definitionen berücksichtigt werden.

SYS.1.7.A8 Einsatz des z/OS-Sicherheitssystems RACF (B)

Der Einsatz von RACF für z/OS MUSS sorgfältig geplant werden, dazu gehören auch die Auswahl des Zeichensatzes, die Festlegung von Regeln für User-ID und Passwort sowie die Aktivierung der KDFAES-Verschlüsselung. Falls RACF PassTickets verwendet werden, MUSS der Enhanced PassTicket Algorithmus aktiviert werden. Voreingestellte Passwörter für das RVARY-Kommando und für neu angelegte User-IDs MÜSSEN geändert werden. Falls RACF-Exits eingesetzt werden sollen, MUSS deren Einsatz begründet, dokumentiert und regelmäßig überwacht werden.

Für das Anlegen, Sperren, Freischalten und Löschen von RACF-Kennungen MÜSSEN geeignete Vorgehensweisen festgelegt sein. Nach einer festgelegten Anzahl fehlgeschlagener Anmeldeversuche MUSS eine RACF-Kennung gesperrt werden (Ausnahme: Notfall-User-Verfahren). Kennungen von

Benutzenden MÜSSEN außerdem nach längerer Inaktivität gesperrt werden, Kennungen von Verfahren hingegen nicht.

Dateien, Started Tasks und sicherheitskritische Programme MÜSSEN mittels RACF-Profilen geschützt werden. Benutzende DÜRFEN darüber NUR die Zugriffsmöglichkeiten erhalten, die sie gemäß ihrer Rolle benötigen. Es MUSS außerdem sichergestellt sein, dass Benutzende ihre Zugriffsmöglichkeiten nicht unerlaubt erweitern können.

SYS.1.7.A9 Mandantenfähigkeit unter z/OS (B)

Falls ein z/OS-System von Mandanten genutzt werden soll, MUSS ein RACF-Konzept zur Mandantentrennung erstellt werden. Die Daten und Anwendungen der Mandanten MÜSSEN durch RACF-Profile getrennt werden. Hohe Berechtigungen im RACF (SPECIAL, OPERATIONS, AUDITOR) und ändernden Zugriff auf Dateien des z/OS-Betriebssystems DÜRFEN NUR Mitarbeitende der Betreibenden haben. Die Wartungsfenster, in denen das z/OS-System nicht zur Verfügung steht, MÜSSEN mit allen Mandanten, die auf dem betroffenen System arbeiten, abgestimmt werden.

SYS.1.7.A10 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.7.A11 Schutz der Session-Daten (B)

Session-Daten für die Verbindungen der RACF-Administrierenden und möglichst auch der anderen Mitarbeitenden MÜSSEN verschlüsselt übertragen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.7.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.7.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.7.A14 Berichtswesen zum sicheren Betrieb von z/OS (S)

Zur Überwachung aller sicherheitsrelevanten Tätigkeiten unter z/OS SOLLTE ein Prozess eingerichtet werden. In diesem SOLLTE festgelegt sein, welche Sicherheitsreports regelmäßig erstellt werden, welche Tools und Datenquellen dabei herangezogen werden (z. B. System Management Facility) und wie mit Abweichungen von den Vorgaben umgegangen wird. Die Sicherheitsreports SOLLTEN bei Überprüfungen als Information verwendet werden.

SYS.1.7.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.7.A16 Überwachung von z/OS-Systemen (S)

Während des Betriebs SOLLTE das z/OS-System auf wichtige Meldungen, Ereignisse und die Einhaltung von Grenzwerten überwacht werden. Insbesondere Fehlermeldungen auf der HMC-Konsole, WTOR- und wichtige WTO-Nachrichten (Write To Operator/with Reply), System Tasks, Sicherheitsverletzungen, Kapazitätsgrenzen sowie die Systemauslastung SOLLTEN berücksichtigt werden. Für die Überwachung SOLLTEN außerdem mindestens die MCS-Konsole, die System Management Facility, das SYSLOG und die relevanten Protokolldaten der Anwendungen herangezogen werden. Es SOLLTE gewährleistet sein, dass alle wichtigen Meldungen zeitnah erkannt werden und, falls notwendig, in geeigneter Weise darauf reagiert wird. Systemnachrichten SOLLTEN dabei so gefiltert werden, dass nur die wichtigen Nachrichten dargestellt werden.

SYS.1.7.A17 Synchronisierung von z/OS-Passwörtern und RACF-Kommandos (S)

Falls z/OS-Passwörter oder RACF-Kommandos über mehrere z/OS-Systeme automatisch synchronisiert werden sollen, SOLLTEN die jeweiligen Systeme möglichst weitgehend standardisiert sein. Die Sperrung von Kennungen durch Fehleingaben von Passwörtern SOLLTE NICHT synchronisiert werden. Das Risiko durch Synchronisation sicherheitskritischer RACF-Kommandos SOLLTE berücksichtigt werden. Die Verwaltungsfunktion des Synchronisationsprogramms SOLLTE nur autorisierten Mitarbeitenden im Rahmen ihrer Tätigkeit zur Verfügung stehen.

SYS.1.7.A18 Rollenkonzept für z/OS-Systeme (S)

Mindestens für die Systemverwaltung von z/OS-Systemen SOLLTE ein Rollenkonzept eingeführt werden. Für alle wichtigen Rollen der Systemverwaltung SOLLTEN außerdem Stellvertretungsregelungen vorhanden sein. Die RACF-Attribute SPECIAL, OPERATIONS und AUDITOR SOLLTEN verschiedenen Personen zugeordnet werden (Rollentrennung).

SYS.1.7.A19 Absicherung von z/OS-Transaktionsmonitoren (S)

Falls Transaktionsmonitore oder Datenbanken unter z/OS eingesetzt werden, wie beispielsweise IMS, CICS oder Db2, SOLLTEN diese mittels RACF abgesichert werden. Dies gilt auch für die zugehörigen System-Kommandos und -Dateien. Interne Sicherheitsmechanismen der Transaktionsmonitore und Datenbanken SOLLTEN hingegen nur dort angewandt werden, wo es keine entsprechenden RACF-Funktionen gibt. Benutzende und Administrierende SOLLTEN nur die Zugriffsrechte erhalten, die sie für ihre jeweilige Tätigkeit benötigen.

SYS.1.7.A20 Stilllegung von z/OS-Systemen (S)

Bei der Stilllegung von z/OS-Systemen SOLLTEN andere z/OS-Systeme, Verbünde und Verwaltungssysteme so angepasst werden, dass sie nicht mehr auf das stillgelegte System verweisen. Auch die Auswirkungen auf die Software-Lizenzen SOLLTEN berücksichtigt werden.

Datenträger, die vertrauliche Daten enthalten, SOLLTEN so gelöscht werden, dass ihr Inhalt nicht mehr reproduziert werden kann. Für den Fall, dass defekte Datenträger durch das herstellende Unternehmen ausgetauscht werden, SOLLTE vertraglich vereinbart sein, dass diese Festplatten sicher vernichtet oder so gelöscht werden, dass ihr Inhalt nicht mehr reproduziert werden kann.

SYS.1.7.A21 Absicherung des Startvorgangs von z/OS-Systemen (S)

Die für den Startvorgang eines z/OS-Systems notwendigen Parameter SOLLTEN dokumentiert und dem Operating-Personal bekannt sein. Außerdem SOLLTEN die erforderlichen Hardware-Konfigurationen vorliegen, wie die IOCDS-Datei (Input/Output Configuration Data Set) und die LPARs (Logical Partitions). Eine z/OS-Master-Konsole und eine Backup-Konsole SOLLTEN definiert sein, um Nachrichten kontrollieren zu können. Nach dem Startvorgang SOLLTE anhand einer Prüfliste kontrolliert werden, ob der Systemstatus den Soll-Vorgaben entspricht. Darüber hinaus SOLLTE eine Fallback-Konfiguration vorgehalten werden, mit der das System vor der letzten Änderung erfolgreich gestartet worden ist.

SYS.1.7.A22 Absicherung der Betriebsfunktionen von z/OS (S)

Alle die Produktion beeinflussenden Wartungsarbeiten sowie dynamische und sonstige Änderungen SOLLTEN nur im Rahmen des Änderungsmanagements durchgeführt werden (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*). SDSF (System Display and Search Facility) und ähnliche Funktionen sowie die Prioritäten-Steuerung für Jobs SOLLTEN mittels RACF vor unberechtigtem Zugriff geschützt werden. z/OS-System-Kommandos und besonders sicherheitsrelevante Befehle für dynamische Änderungen SOLLTEN über RACF geschützt werden. Bei der dynamischen Definition von Hardware SOLLTE sichergestellt werden, dass eine Ressource im Wirkbetrieb nicht mehreren Einzelsystemen außerhalb eines Parallel Sysplex zugeordnet wird.

SYS.1.7.A23 Absicherung von z/VM (S)

Falls z/VM eingesetzt wird, SOLLTE das Produkt in das Patch-Management integriert werden. Alle voreingestellten Passwörter SOLLTEN geändert werden. Die Rolle des z/VM-Systemadministrierenden SOLLTE nur an Personen vergeben werden, die diese Berechtigungen benötigen. Die Sicherheitsadministration von z/VM SOLLTE über RACF für z/VM erfolgen. Passwörter von realen *Usern* und *Guest-Usern* SOLLTEN mittels RACF für z/VM verschlüsselt werden. Die sicherheitskritischen Systemkommandos von z/VM SOLLTEN über RACF geschützt werden. Unter z/VM definierte virtuelle Maschinen SOLLTEN nur die für die jeweiligen Aufgaben notwendigen Ressourcen erhalten und strikt voneinander getrennt sein. Unter z/VM SOLLTEN nur die benötigten Dienste gestartet werden. Wenn Überprüfungen durchgeführt werden, SOLLTEN die Journaling-Funktion von z/VM und die Audit-Funktionen von RACF eingesetzt werden.

SYS.1.7.A24 Datenträgerverwaltung unter z/OS-Systemen (S)

Dateien, Programme und Funktionen zur Verwaltung von Datenträgern sowie die Datenträger selbst (Festplatten und Bänder) einschließlich Master-Katalog SOLLTEN mittels RACF-Profilen geschützt werden. Es SOLLTEN Sicherungskopien aller wichtigen Dateien zur Verfügung stehen, die in einer Notfallsituation zurückgespielt werden können. Die Zuordnung von Datenträgern zu den Z-Systemen SOLLTE nachvollziehbar sein. Es SOLLTE gewährleistet werden, dass je nach Volumen und Zeitfenster genügend Bandstationen zur Verfügung stehen. Beim Einsatz des HSM (Hierarchical Storage Manager) SOLLTE festgelegt werden, welche Festplatten gesichert werden sollen und wie die Sicherung erfolgen soll. Bänder, die vom HSM verwaltet werden, SOLLTEN NICHT anderweitig bearbeitet werden.

SYS.1.7.A25 Festlegung der Systemdimensionierung von z/OS (S)

Die Grenzen für die maximale Belastung der Ressourcen (Anzahl der CPUs, Speicher, Bandbreite etc.) SOLLTEN den Hardware-Voraussetzungen entsprechend festgelegt und den zuständigen Administrierenden und Anwendungszuständigen bekannt sein. Die Anzahl der zur Verfügung stehenden Magnetband-Stationen, die Zeiten, zu denen Anwendungen auf Magnetband-Stationen zugreifen und die benötigten Festplattenkapazitäten SOLLTEN mit den Anwendungszuständigen abgestimmt sein. Die Festplattenkapazitäten SOLLTEN außerdem vom Space-Management überwacht werden.

SYS.1.7.A26 WorkLoad Management für z/OS-Systeme (S)

Die Programme, Dateien und Kommandos des WorkLoad Managers (WLM) sowie die dafür notwendigen Couple Data Sets SOLLTEN mittels RACF geschützt werden. Dabei SOLLTE sichergestellt sein, dass die Berechtigungen zum Ändern des WLM über z/OS-Kommandos und über die SDSF-Schnittstelle gleich sind.

SYS.1.7.A27 Zeichensatzkonvertierung bei z/OS-Systemen (S)

Wenn Textdateien zwischen z/OS-Systemen und anderen Systemen übertragen werden, SOLLTE darauf geachtet werden, dass eventuell eine Zeichensatzkonvertierung erforderlich ist. Dabei SOLLTE die korrekte Umsetzungstabelle verwendet werden. Bei der Übertragung von Programm-Quellcode SOLLTE geprüft werden, ob alle Zeichen richtig übersetzt wurden. Bei der Übertragung von Binärdaten SOLLTE hingegen sichergestellt sein, dass keine Zeichensatzkonvertierung stattfindet.

SYS.1.7.A28 Lizenzschlüssel-Management für z/OS-Software (S)

Für Lizenzschlüssel, deren Gültigkeit zeitlich begrenzt ist, SOLLTE ein Verfahren zur rechtzeitigen Erneuerung eingerichtet sein. Die Laufzeiten der Lizenzschlüssel SOLLTEN dokumentiert werden. Die Dokumentation SOLLTE allen betroffenen Administrierenden zur Verfügung stehen.

SYS.1.7.A29 Absicherung von Unix System Services bei z/OS-Systemen (S)

Die Parameter der Unix System Services (USS) SOLLTEN entsprechend der funktionalen und sicherheitstechnischen Vorgaben sowie unter Berücksichtigung der verfügbaren Ressourcen eingestellt werden. HFS- und zFS-Dateien, die USS-Dateisysteme enthalten, SOLLTEN über RACF-Profile

abgesichert und in das Datensicherungskonzept einbezogen werden. Außerdem SOLLTE das Root-Dateisystem mit der Option Read-Only gemounted werden. Es SOLLTE im USS-Dateisystem KEINE APF-Autorisierung (Authorized Program Facility) über das File Security Packet (FSP) geben. Stattdessen SOLLTEN die Module von APF-Dateien des z/OS-Betriebssystems geladen werden. Zwischen USS-User-IDs und z/OS-User-IDs SOLLTE es eine eindeutige Zuordnung geben. Berechtigungen unter USS SOLLTEN über die RACF-Klasse UNIXPRIV vergeben werden und NICHT durch Vergabe der UID 0. Für Überprüfungen und das Monitoring der USS SOLLTEN die gleichen Mechanismen wie für z/OS genutzt werden.

SYS.1.7.A30 Absicherung der z/OS-Trace-Funktionen (S)

Die Trace-Funktionen von z/OS wie GTF (Generalized Trace Facility), NetView oder ACF/TAP (Advanced Communication Function/Trace Analysis Program) und die entsprechenden Dateien SOLLTEN so geschützt werden, dass nur die zuständigen und autorisierten Mitarbeitenden darauf Zugriff haben. Die Trace-Funktion von NetView SOLLTE deaktiviert sein und nur im Bedarfsfall aktiviert werden.

SYS.1.7.A31 Notfallvorsorge für z/OS-Systeme (S)

Es SOLLTE ein Verfahren zur Wiederherstellung einer funktionierenden RACF-Datenbank vorgesehen sein. Weiterhin SOLLTEN eine Kopie des z/OS-Betriebssystems als z/OS-Backup-System und, unabhängig von Produktivsystem, ein z/OS-Notfallsystem vorgehalten 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.

SYS.1.7.A32 Festlegung von Standards für z/OS-Systemdefinitionen (H)

Es SOLLTEN Standards und Namenskonventionen für z/OS-Systemdefinitionen festgelegt und dokumentiert werden. Die Dokumentationen SOLLTEN den Administrierenden zur Verfügung stehen. Die Einhaltung der Standards SOLLTE regelmäßig überprüft werden. Standards SOLLTEN insbesondere für Datei-, Datenbank-, Job- und Volume-Namen sowie für Application-, System- und User-IDs definiert werden.

SYS.1.7.A33 Trennung von Test- und Produktionssystemen unter z/OS (H)

Es SOLLTEN technische Maßnahmen ergriffen werden, um Entwicklungs- und Testsysteme von Produktionssystemen unter z/OS zu trennen. Dabei SOLLTEN eventuelle Zugriffsmöglichkeiten über gemeinsame Festplatten und den Parallel Sysplex beachtet werden.

SYS.1.7.A34 Batch-Job-Planung für z/OS-Systeme (H)

Wenn ein z/OS-System eine größere Anzahl von Batch-Jobs verarbeitet, SOLLTE für die Ablaufsteuerung der Batch-Jobs ein Job-Scheduler eingesetzt werden. Der Job-Scheduler sowie die zugehörigen Dateien und Tools SOLLTEN mittels RACF geeignet geschützt werden.

SYS.1.7.A35 Einsatz von RACF-Exits (H)

Falls RACF-Exits eingesetzt werden, SOLLTEN die sicherheitstechnischen und betrieblichen Auswirkungen analysiert werden. Die RACF-Exits SOLLTEN außerdem über das SMP/E (System Modification Program/Enhanced) als USERMOD installiert und überwacht werden.

SYS.1.7.A36 Interne Kommunikation von Betriebssystemen (H)

Die Kommunikation von Betriebssystemen, z/OS oder Linux, die entweder im LPAR-Mode oder unter z/VM auf derselben Z-Hardware installiert sind, SOLLTE über interne Kanäle erfolgen, d. h. über HiperSockets oder virtuelle CTC-Verbindungen (Channel-to-Channel).

SYS.1.7.A37 Parallel Sysplex unter z/OS (H)

Anhand der Verfügbarkeits- und Skalierbarkeitsanforderungen SOLLTE entschieden werden, ob ein Parallel Sysplex (Cluster von z/OS-Systemen) eingesetzt wird und gegebenenfalls welche Redundanzen dabei vorgesehen werden. Bei der Dimensionierung der Ressourcen SOLLTEN die Anforderungen der Anwendungen berücksichtigt werden. Die Software und die Definitionen der LPARs des Sysplex, einschließlich RACF, SOLLTEN synchronisiert oder als gemeinsam benutzte Dateien bereitgestellt sein.

Es SOLLTE sichergestellt sein, dass alle LPARs des Sysplex auf die Couple Data Sets zugreifen können. Die Couple Data Sets sowie alle sicherheitskritischen Programme und Kommandos zur Verwaltung des Sysplex SOLLTEN mittels RACF geschützt werden. Außerdem SOLLTE ein GRS-Verbund (Global Resource Serialization) eingerichtet werden. Die Festplatten des Sysplexes SOLLTEN strikt von den Festplatten anderer Systeme getrennt werden. Der System Logger SOLLTE mit Staging Data Set eingesetzt werden.

SYS.1.7.A38 Einsatz des VTAM Session Management Exit unter z/OS (H)

Falls ein VTAM Session Management Exit eingesetzt werden soll, SOLLTE gewährleistet werden, dass dadurch der sichere und performante Betrieb nicht beeinträchtigt wird. Der Exit SOLLTE mindestens eine nachträgliche Kontrolle der abgewiesenen Login-Versuche ermöglichen. Außerdem SOLLTE sich der Exit dynamisch konfigurieren lassen und das Regelwerk von einer externen Datei nachladen. Funktionen, Kommandos und Dateien im Zusammenhang mit dem Exit SOLLTEN durch RACF geschützt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Im Umfeld von Z-Systemen sind eine Reihe von Abkürzungen gebräuchlich, die nicht an anderen Stellen im IT-Grundschutz erläutert werden. Hierzu gehören:

- HMC (Hardware Management Console), MCS (Multiple Console Support), SMCS, Extended MCS: Konsolen zur Steuerung und Kontrolle eines Z-Systems bzw. z/OS-Betriebssystems
- HFS: Hierarchical File System, Hierarchisches Dateisystem
- IPL: Initial Program Load, Startvorgang eines Betriebssystems
- RSF: Remote Support Facility
- SE: Support Elements, zur Konfiguration und Kontrolle des Systems
- SMP/E: System Modification Program/Extended, Verfahren zur Software-Installation
- zFS: zSeries File System, Dateisystem, das unter z/OS und Unix System Services (USS) eingesetzt wird.

Der Hersteller IBM gibt weitere Informationen zum Thema IBM Z in „ABC of z/OS System Programming Volume 1-13“, IBM Redbooks, https://www.redbooks.ibm.com.