Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein SYS.1.7 IBM Z

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 IBM Z-Architektur ist der Nachfolger der 1964 eingeführten S/360-Architektur und wird bei heutigen Großrechner-Installationen häufig eingesetzt.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.1.7 *IBM Z* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein SYS.1.7 IBM Z

SYS.1.7.M1 Einsatz restriktiver z/OS-Kennungen (B)

Übersicht über die RACF-Attribute SPECIAL, OPERATIONS, AUDITOR
Um einen Überblick zu erhalten, welche Benutzenden spezielle RACF–Attribute wie SPECIAL, OPERATIONS, AUDITOR haben, kann beispielsweise der Data Security Monitor (DSMON) genutzt werden.

Der „Selected user attribute summary report“ liefert eine Auflistung aller Benutzenden, die eines der oben aufgeführten Attribute auf System- oder auch Gruppenebene haben. Diese Information ist auch über andere Tools oder Zusatzprodukte erhältlich. Diese Übersicht sollte regelmäßig erstellt und überprüft werden.

Übersicht über Benutzende mit UID 0

Um eine Übersicht zu erhalten, welchen Benutzenden die UID 0 zugeordnet wurde, kann beispielsweise der Search-Befehl „SEARCH CLASS(USER) UID(0)“ genutzt werden.

Es sollte geprüft werden, ob wirklich UID 0 zwingend notwendig ist, oder ob alternativ über Profile aus der Klasse UNIXPRIV die notwendigen Berechtigungen vergeben werden können.

RACF Health Check: RACF_IBMUSER_REVOKED

Um sicher zu stellen, dass die Kennung IBMUSER nicht benutzt werden kann, gibt es einen von IBM gelieferten Health Check „RACF_IBMUSER_REVOKED“. Dieser Check überprüft, ob die Kennung IBMUSER gesperrt ist. Falls die Kennung nicht gesperrt ist, erfolgt eine Alarmierung. Diese Überprüfung sollte eingeschaltet sein und kann bei Bedarf auf eigene spezifische Kennungen erweitert werden.

SYS.1.7.M2 Absicherung sicherheitskritischer z/OS-Dienstprogramme (B)

Schutz von sicherheitskritischen (Dienst-)Programmen und Kommandos

Der Programmschutz ist über Profile in der Klasse PROGRAM möglich. Für sicherheitskritische (Dienst-)Programme und Kommandos sollten entsprechende Profile in der Klasse PROGRAM definiert sein. Über READ oder NONE kann Zugriff auf Programme ermöglicht oder eingeschränkt werden.

Über die erweiterte Programmkontrolle sollte verhindert werden, dass Programme kopiert oder der Inhalt von Programmen angezeigt werden kann.

Zudem sollte die Möglichkeit geprüft werden, Zugriff auf einen Datensatz nur zuzulassen, wenn ein bestimmtes Programm verwendet wird.

Überprüfung der Programme im Program Property Table Report

Der Report „Program Property Table“ des Data Security Monitors (DSMON) zeigt an, welche Programme durch Eintrag in die „Program Property Table“ berechtigt sind, den Passwortschutz zu umgehen, und welche Programme in einem System Key laufen. Programme mit System Key benötigen keine RACF-Autorisierung für die Nutzung von Callable Services. Der Report sollte regelmäßig ausgeführt und überprüft werden.

Die Parameter NOPASS oder NOPASS_ALLOWBATCH geben an, dass kein Sicherheitsschutz erforderlich ist. Es sollten hier nur selektive und bekannte Programme, wie z. B. Kommunikations- und Datenbanksteuerprogramme oder andere Systemsteuerprogramme, definiert sein.

z/OS Health Checker – Check: RACF_SENSITIVE_RESOURCES

Der z/OS Health Checker (siehe SYS.1.7.M4 *Schulung des z/OS-Bedienungspersonals*) bietet einen Check namens RACF_SENSITIVE_RESOURCES.

Dieser Check untersucht die Sicherheitsmerkmale mehrerer systemkritischer Dateien, z. B. der von APF-Dateien (Authorized Program Facility) und allgemeiner Ressourcen. Er überprüft den Schutz jeder Ressource, indem das entsprechende RACF-Profil extrahiert und untersucht wird bzgl. UACC, WARNING-Status und ID(*)-Eintrag in der Zugriffsliste, falls vorhanden. Außerdem markiert der Check eine Datei als Ausnahme, wenn es kein zuständiges Profil gibt, das eine Datei schützt, und wenn NOPROTECTALL oder PROTECTALL(WARN) als Optionen gesetzt sind.

Dieser Check sollte regelmäßig ausgeführt werden. Es wird empfohlen, auf die vom Health Checker aufgeführten Ausnahmen zu reagieren und die Einstellungen entsprechend anzupassen.

Schwachstellenanalyse für autorisierte Programme

Der IBM z/OS Authorized Code Scanner (zACS) ist ein optionales kostenpflichtiges Feature von z/OS, das automatisierte Systemintegritätstests durchführt. Er sucht nach Program Calls (PCs) und Supervisor Calls (SVCs), überprüft diese dynamisch auf Integrität und deckt damit potenzielle Schwachstellen auf.

Es sollte entschieden werden, ob der z/OS Authorized Code Scanner eingesetzt werden soll. Falls er eingesetzt wird, sollten neue bzw. geänderte Programme damit überprüft werden, bevor sie produktiv werden. Die Ausgabe des Scanners sollte ausgewertet werden, um etwaige potenzielle Schwachstellen zu erkennen und anschließend zu beheben.

SYS.1.7.M3 Wartung von Z-Systemen (B)

Die Wartung von Z-Systemen betrifft nicht nur die eigentliche Hardware, sondern auch die Firmware und die Betriebssysteme. Dabei spielt die Hardware Management Console (HMC) eine wichtige Rolle. Daher werden in dieser Maßnahme auch Sicherheitsaspekte der HMC behandelt. Weitere Hinweise zur Sicherheit von Konsolen/Terminals finden sich in SYS.1.7.M5 *Einsatz und Sicherung systemnaher z/OS-Terminals*.

Weil es kontinuierlich Erweiterungen, Verbesserungen und Korrekturen an den z/OS-Komponenten gibt, die IBM als sog. „Continuous Delivery“ bereitstellt, liegt es in der Verantwortung der Administrierenden, sich darüber zu informieren und gegebenenfalls diese Updates zu implementieren.

Hardware

Die Grundlage für Schutz der Daten und deren Verarbeitung ist PR/SM als Licensed Internal Code (LIC), der alle installierten und aktivierten Ressourcen der IBM zSystems Plattform als ein einzelnes großes symmetrisches Multiprozessor (SMP)-System verwaltet und virtualisiert. Diese Virtualisierung bietet Sicherheitsfunktionen und erlaubt das Teilen der installierten Ressourcen.

Der Secure Service Container (SSC) ist eine darauf aufbauende integrierte IBM zSystems Appliance in Form eines separaten und speziellen LPAR-Typs mit besonderen Schutzfunktionen in den Bereichen Hauptspeicher, Netze und Daten (in Transit und beim Speichern).

CP Assist for Cryptographic Function (CPACF) als kostenloses Hardware-Feature (FC#3863) sollte immer aktiviert werden. CPACF bietet den vollen Umfang des Advanced Encryption Standard (AES) und der Secure-Hash-Algorithmen (SHA-2). Die Nutzung von CPACF ist durch eine Gruppe von Message-Security Assist (MSA) Instruktionen implementiert und wird automatisch zur Beschleunigung der aufgeführten Algorithmen verwendet.

IBM zSystems Kryptographische Co-Prozessoren (Crypto Express Adapter) sind eine optionale und kostenpflichtige Erweiterung der jeweiligen IBM zSystems Server Generation. Crypto Express Adapter sind entwickelt worden, um die kryptographischen Fähigkeiten der CPACF Unterstützung zu erweitern, um weitere Algorithmen, Signatur- und Secure-Key-Verfahren für den noch besseren Schutz von transferierten und gespeicherten Daten zu unterstützen.

Hardware Management Console (HMC)

Die Hardware Management Console (HMC) verwaltet und steuert die IBM zSystems Plattform. Sie ist als eine Art Appliance zu betrachten, deren Zweck das zentrale Management und Steuerung aller IBM zSystems Ressourcen sowie installierter Betriebssysteme und angeschlossener Peripherie über ein grafisches Bedieninterface ist. Zusätzlich können mittels der HMC das SNMP und WebServices auf der Grundlage standardisierter Protokolle für Auditierungszwecke automatisiert werden. Deshalb ist die HMC als kritische Komponente zu bewerten und in einem gesicherten Setup und zutrittskontrollierten Umfeld zu betreiben. Im Folgenden wird beschrieben, welche Sicherheitsfunktionen zur Verfügung stehen und wie sie konfiguriert werden können, um den Sicherheitsanforderungen eines Anwendenden zu entsprechen.

Die HMC ist eine geschlossene Plattform. Das bedeutet, Benutzende haben keinen Zugriff auf das Betriebssystem und sind auch nicht in der Lage, andere Applikationen auf diesem System zu betreiben.

Alle Funktionen und Konfigurationen der HMC werden durch vordefinierte Tasks des installierten HMC Licensed Internal Code zur Verfügung gestellt.

Die HMC bietet einen kompletten Satz von Profilen, über die die Funktionen und Rechte der HMC-Benutzenden gesteuert, kontrolliert und protokolliert werden können. Darüber hinaus sollten Funktionen aktiviert werden, die inaktive Benutzende automatisch abmelden und die Benutzenden zur Einhaltung starker Passwortregeln zwingen.

Die HMC User Management Task unterstützt die Nutzung einer Multi-Faktor-Authentisierung mittels:

- RSA SecurID (AZFSIDP1)
- Generic RADIUS (AZFRADP1)
- Certificate authentication (AZFCERT1)

Der HMC Licensed Internal Code beinhaltet eine voll funktionale Firewall für die Beschränkung und Kontrolle des Netzzuganges, die standardmäßig keinen eingehenden Netzzugriff erlaubt. Sofern bestimmte Funktionen der HMC explizit und durch berechtige Administrierende erlaubt werden (bspw. Fernzugriff, SNMP-basierende Automation, Web Services Automation), werden die dafür notwendigen eingehenden Protokolle erlaubt.

Sowohl die HMC als auch das Support Element (SE) unterstützen TLS-Protokolle (Transport Layer Security) für sichere Kommunikation, die bspw. für Fernzugriff und Verbindungen zum IBM Service Support System (RSF) empfohlen bzw. notwendig sind.

Für die ausgehende Verbindung zum IBM Service Support System (RSF) muss die Firewall des Anwenders den entsprechenden Datenverkehr zu „esupport.ibm.com" auf Port 443 erlauben.

Für das Weiterleiten von TLS-Sockets über einen Proxy-Server muss der Parameter „Use SSL Proxy Connection to Internet“ gesetzt werden. Außerdem müssen die IP-Adresse und die Port-Nummer des Proxy-Servers angegeben werden.

Es sollten nur kryptographische Algorithmen und Protokolle in der Konfiguration erlaubt werden, die aktuellen Sicherheitsstandards entsprechen. Damit Cipher Suites zur Verfügung stehen, die aktuellen Sicherheitsstandards entsprechen, sollten die Microcode Level (MCL) der SE und HMC auf einem aktuellen Stand gehalten werden.

Die HMC bietet auch eine Reihe von Mechanismen zum Schutz gegen Schadprogramme.

IBM gewährleistet den Schutz aller HMC/SE Licensed Internal Code (LIC) Updates, auch als Firmware Updates bekannt, durch digital signierte Firmware.

Ergänzend wird empfohlen, für alle Dateiübertragungen gesicherte FTP-Verbindungen zu benutzen, unterstützt werden FTPS (FTP Secure) und SFTP (SSH FTP).

Mit Hilfe der Audit und Log Management Task können Audit Reports generiert, angesehen, gespeichert und weitergeleitet (bspw. an ein SIEM) werden. Folgende HMC und SE Reports können für die Verwendung bei Audits bereitgestellt werden:

- Console event log
- Console service history
- Tasks performed log
- Security logs
- System log.

Durch Einstellungen in der Scheduled Operations Task können die Auditaktivitäten automatisiert werden.

Über die Monitor System Events Task sollten alle Security Logs und E-Mail-Benachrichtigungen mit denselben Filtern und Regeln generiert werden, wie sie für Hardware- und Betriebssystem-Messages gelten.

Voraussetzung einer konsequenten Umsetzung der Sicherheit ist aber auch, die HMC sowohl in einer physisch gesicherten (zutrittskontrollierten) Umgebung als auch in einem gesicherten Netzbereich zu platzieren.

Wartung (Preventive Service Planning)

IBM stellt in einer Preventive Maintenance Planning Database in Form von sogenannten PSP buckets spezifische Hinweise zu Hardware-Installationen und Upgrades, zu erwartenden Problemen mit hoher Auswirkung und Service-Empfehlungen zur Verfügung. Diese Hinweise können auf folgender Website abgerufen werden: https://esupport.ibm.com/customercare/psearch/search?domain=psp

Die Informationen betreffen sowohl Software als auch Hardware der IBM zSystems Plattform und werden nach individuell einstellbaren Filtern zur Verfügung gestellt.

IBM Z und LinuxONE Security Portal

Das IBM Z und LinuxONE Security Portal enthält Sicherheits-/Integritäts-Informationen (APARs) für die Betriebssysteme z/OS und z/VM und zugehörige IBM-Produkte sowie kritische Sicherheitshinweise bezüglich Hardware-, Firmware- und Softwareproblemen. Diese werden nicht allgemein veröffentlicht, sondern registrierten Anwendenden und autorisierten Personen nur über das IBM Z und LinuxONE Security Portal zur Verfügung gestellt.

Das IBM Z und LinuxONE Security Portal bietet einen kontrollierten Benachrichtigungs- und Verteilungsmechanismus, um sicherzustellen, dass diese kritischen Informationen nur denjenigen Anwendenden von IBM zSystems zur Verfügung stehen, die davon wissen müssen, ohne dass Informationen veröffentlicht werden, die Ihre Systeme in Gefahr bringen könnten.

Anwendenden wird empfohlen, sich auf folgender Website für das IBM Z und LinuxONE Security Portal zu registrieren: https://www-03.ibm.com/systems/campaignmail/z/capabilities/system-integrity/register-zsecurity-portal

SYS.1.7.M4 Schulung des z/OS-Bedienungspersonals (B)

In Ergänzung zur notwendigen Basisausbildung gibt es einige Hilfsfunktionen, die die Administration eines z/OS-Systems vereinfachen.

z/OS Health Checker

Der z/OS Health Checker ist eine Basisfunktion, die das Ziel hat, potenzielle Probleme zu identifizieren, bevor diese die Verfügbarkeit beeinträchtigen oder sogar zu Systemausfällen führen. Das laufende System wird überprüft und die aktiven Sysplex-Definitionen und Einstellungen werden mit den von IBM vorgeschlagenen Werten verglichen. Abweichungen werden in Form von detaillierten Meldungen dokumentiert.

Health Checks, also Systemüberprüfungen, gibt es für zahlreiche Komponenten, und es besteht die Möglichkeit, die Überprüfungen auf die Bedürfnisse der Institution anzupassen oder auch eigene Systemprüfungen zu erstellen.

Es wird empfohlen, auf die vom Health Checker aufgeführten Meldungen zu reagieren und die Einstellungen entsprechend anzupassen.

IBM z/OS Management Facility (z/OSMF)

IBM z/OS Management Facility (z/OSMF) bietet Systemverwaltungsfunktionen in einer aufgabenorientierten, webbrowserbasierten Bedienoberfläche mit integrierter Unterstützung für Benutzende, sodass der tägliche Betrieb und die Administration von z/OS Systemen vereinfacht werden kann. Dazu gehören auch Funktionen zur Rationalisierung und Automatisierung.

z/OSMF kann als zentraler Kontrollpunkt genutzt werden für:

- Anzeigen, Definieren und Aktualisieren von Richtlinien, die sich auf das Systemverhalten auswirken
- Überwachung der Leistung der Systeme

- Verwaltung der z/OS-Software
- Verwaltung von Problemdaten
- Konsolidierung der z/OS-Verwaltungstools.

Außerdem besteht die Möglichkeit, eigene Arbeitsabläufe zu definieren.

Security Configuration Assistant

Der „Security Configuration Assistant" ist eine Komponente vom z/OSMF, mit der sich überprüfen lässt, ob die Sicherheitseinstellungen für das z/OSMF-Hostsystem und seine Benutzenden ordnungsgemäß konfiguriert ist. Autorisierungen für z/OSMF selbst können überprüft werden, einschließlich des Nucleus, der Basis und optionalen Dienste sowie der erweiterten Konfigurationsoptionen. Es lassen sich auch die Sicherheitseinstellungen für andere Produkte auf dem System überprüfen, für die die Sicherheitsbeschreibungsdateien verfügbar sind.

SYS.1.7.M5 Einsatz und Sicherung systemnaher z/OS-Terminals (B)

Für Umsetzungshinweise zu Support Elements (SE) und zur Hardware Management Console (HMC) wird auf die Maßnahme SYS.1.7.M3 *Wartung von z-Systemen* verwiesen.

Integrated Console Controller (ICC)

OSA-ICC (Open Systems Adapter - Integrated Console Controller) stellt einen TN3270E-Zugang als Nicht-SNA-Verbindung bereit. OSA-ICC-3270-Sessions werden gebraucht für das IPL logischer Partitionen innerhalb eines Channel Subsystems (CSS) und stellen zusätzlich eine System-Operator/Master-Konsole für z/OS, z/VM und z/VSE bereit. Die definierten OSA-ICC Sessions können auch für TSO-, VM-, oder VSE-Systemprogrammierer als standardmäßige TN3270E-Konsole genutzt werden. Jeder OSA-ICC-Adapter kann maximal 120 Sessions über TCP/IP für Workstations bereitstellen, auf denen ein TN3270E-Emulator gemäß RFC 2355 läuft.

Seit der Generation IBM z13 GA2 unterstützt OSA-ICC auch maximal 48 sichere Verbindungen pro Adapter basierend auf Transport Layer Security (TLS). Bei TLS werden die Kommunikationspartner über X.509-Zertifikate authentisiert. Die Zertifikate können dabei sowohl pro PCHID als auch pro Z-System genutzt werden. Die Konfiguration der TLS-Verbindung sollte gemäß den allgemeinen Vorgaben der Institution (vgl. CON.1.A1 *Auswahl geeigneter kryptografischer Verfahren*) erfolgen.

TLS wird von neuen Versionen des IBM Personal Communications Emulators (PCOMM) unterstützt. Für andere TN3270E-Emulatoren ist die Unterstützung beim Hersteller zu prüfen.

Die Nutzung eines OSA-ICC als 3270 Control Unit muss zunächst über die Hardware Management Console (HMC) und das Support Element (SE) konfiguriert werden.

Master Console Service (MCS)

Standardmäßig ist nach wie vor die Nutzung eines Passwortes zwingend erforderlich. Seit z/OS V2R2 und V2R3 (APAR OA54790) unterstützt die Master-Konsole alternativ zu einem 8 Zeichen langen Passwort auch ein Login mittels Passphrase (maximal 45 Zeichen).

Um Operatoren das Login mittels Passphrase zu ermöglichen, muss der RACF-Administrierende diese Funktion aktivieren. Wenn das Profil MVS.CONSOLE.PASSWORDPHRASE.CHECK in der Klasse OPERCMDS des Security-Produktes (RACF oder äquivalent) definiert ist, wird die Nutzung einer MCS Operator Password Phrase aktiviert.

Die Verwendung von Passphrasen wird ermittelt, wenn eine Konsole aktiviert oder in den Standby Mode versetzt wird. Sollte der Password-Status im Security-Produkt geändert werden, während die Konsole aktiv ist, wird der bisherige Status beibehalten, bis die Konsole reaktiviert wird.

Das Logon-Kommando akzeptiert eine maximal 45 Zeichen lange Passphrase, eingeschlossen in Hochkommata (bspw. 'Fred Loves Wilma'). Die Hochkommata werden dabei nicht als Teil der Passphrase betrachtet.

Die Nutzung von Passphrasen anstelle von 8-stelligen Passwörtern wird empfohlen. Dabei sind die entsprechenden Regelungen der Institution zu beachten.

Um TSO/E-Konsolen als extended MCS-Konsole benutzen zu können, wird der z/OS Security Server (RACF oder äquivalent) benötigt, weil darüber die Console Security Attribute gesteuert werden.

Die Klasse CONSOLE kontrolliert den Zugriff auf MCS-Konsolen und Ressourcen, die durch Kommandos von der Konsole benutzt werden müssen.

SYS.1.7.M6 Einsatz und Sicherung der Remote Support Facility (B)

Für die Wartung der IBM zSystems Plattform mittels RSF müssen regelmäßig Informationen zwischen Hardware Management Console (HMC) und IBM Service Support System ausgetauscht werden. In Richtung IBM zählen dazu Konfigurationsdaten der Maschine, Zustandsinformationen und Fehlermeldungen. In Richtung Anwendender werden unter anderem Updates für Licensed Internal Code (Driver, MCL, usw.) übertragen.

Um die dafür notwendigen Konfigurationen vornehmen zu können, ist eine Anmeldung an der Hardware Management Console im ACSADMIN- oder SERVICE-Modus erforderlich.

IBM empfiehlt, eine der Ethernet-Verbindungen pro HMC mit dem privaten LAN zwischen HMC, CPC und SE zu konfigurieren. Die zweite ETH-Schnittstelle sollte zum internen Netz verbunden werden und über eine entsprechend konfigurierte Firewall der Institution die Verbindung zum Internet zulassen. Die Firewall der Institution sollte zusätzlich die sogenannte Source Network Address Translation (SNAT) und Maskierungsregeln benutzen, um die IP-Adresse(n) der HMC(s) in den übertragenen Paketen zu verbergen. Außerdem sollte sie die Anzahl der Zieladressen für die HMC begrenzen.

Die Hardware Management Console ist außerdem durch eine interne Firewall geschützt, die standardmäßig nur die Kommunikation der angeschlossenen Server und ausgehende Verbindungen zum IBM Service Support System (esupport.ibm.com auf Port 443) zulässt. In der Standardkonfiguration ist dadurch sichergestellt, dass immer die HMC die Kommunikation zum IBM Service Support System initiieren muss. Das IBM Service Support System wird niemals eine Internetverbindung zur HMC initiieren.

Die interne Firewall der HMC sollte so konfiguriert werden, dass nur die notwendigen Verbindungen (bspw. für Remote Operation der Administrierenden) aufgebaut werden können und alle anderen Verbindungsversuche blockiert werden.

Call Home über gesicherte Verbindung

Sowohl die HMC als auch das Support Element (SE) unterstützen TLS-Protokolle für sichere Kommunikation, die bspw. für Fernzugriff und Call Home (RSF) empfohlen bzw. notwendig sind. Dafür bietet die HMC eine Reihe von Optionen für die Einrichtung einer Breitbandverbindung. Die Sicherheitsfunktionen dienen einerseits der sicheren Kommunikation zwischen HMC und IBM Service Support System, andererseits auch der Integration in das Netz der Institution. Hinweis: Seit HMC Version 2.15.0 wird das bisherige Einwahlverfahren zum IBM Service Support System nicht mehr unterstützt. Ausschließlich wechselseitig authentifizierte TLS-Verbindungen über Breitband-Internet werden unterstützt.

Für die ausgehende Verbindung zum IBM Service Support System (RSF) muss die Firewall des Anwendenden den entsprechenden Datenverkehr zu esupport.ibm.com auf Port 443 erlauben.

Für das Weiterleiten von TLS-Sockets über einen Proxy-Server muss der Parameter „Use SSL Proxy Connection to Internet“ gesetzt werden. Außerdem müssen die IP-Adresse und die Port-Nummer des Proxy-Servers angegeben werden.

Es sollten nur solche kryptographischen Protokolle und Algorithmen konfiguriert werden, die aktuellen Sicherheitsstandards entsprechen. Damit Cipher Suites zur Verfügung stehen, die aktuellen Sicherheitsstandards entsprechen, sollten die Microcode Level (MCL) der SE und HMC auf einem aktuellen Stand gehalten werden.

Eine Checkliste der notwendigen und empfohlenen Konfigurationsoptionen ist zu finden in dem Buch SC28-7026-00 „Integrating the Hardware Management Console's Broadband Remote Support Facility into your Enterprise“ (z16: 26.05.2022).

SYS.1.7.M7 Restriktive Autorisierung unter z/OS (B)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M8 Einsatz des z/OS-Sicherheitssystems RACF (B)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M9 Mandantenfähigkeit unter z/OS (B)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M10 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

SYS.1.7.M11 Schutz der Session-Daten (B)

Die Sicherung von Session-Daten kann sowohl auf der Internet-Schicht zwischen Geräten als auch auf der Transport-Schicht zwischen Clients und Servern von Anwendungen stattfinden. Beiden gemeinsam ist, dass die Session-Partner authentisiert werden müssen (Client-Authentisierung ist auch bei TLS optional) und dass alle während der Session übertragenen Daten verschlüsselt und bezüglich Integrität gesichert werden.

Transport Layer Security (TLS) ist ein Verfahren zum kryptografischen Schutz von Netzverkehr und ist durch die IETF in verschiedenen RFCs definiert. Weil TLS in der Transportschicht implementiert ist, wird sowohl der IP-Header als auch jeglicher UDP-Netzverkehr nicht geschützt. Die Anwendungen (Clients und Server) müssen diese Transportsicherung unterstützen. Ausnahme im z/OS ist die sogenannte Application Transparent TLS (AT-TLS) Implementierung, die auch Anwendungen unterstützt, die die RFCs nicht selbst implementiert haben.

Netzverschlüsselung auf IP-Ebene (IPSec) ist in der Internet-Schicht implementiert, schützt damit auch die IP-Header-Informationen und UDP-Pakete. IPSec ist transparent gegenüber Anwendungen und wird deshalb auch häufig für Virtuelle Private Netze (VPN) oder Tunnel zwischen Geräten und IP-Stacks eingesetzt.

Die dritte Option zum Schutz von Session-Daten ist die Nutzung von SSH. z/OS beinhaltet immer eine aktuelle Version von OpenSSH, mit dessen Hilfe ebenfalls TCP-basierender Datentransfer (bspw. sftp) geschützt werden kann.

z/OSMF Network Configuration Assistant

Die Network Configuration Assistant Task innerhalb des z/OSMF wird benutzt, um Netzressourcen für den z/OS-Betrieb und das IBM Cloud Provisioning and Management für z/OS zu administrieren. Die Funktionalität umfasst:

- Anlegen und Verwalten der Policies für folgende TCP/IP-basierende Aspekte:
    - IP Security, inklusive IKE
    - Network Security Services (NSS)
    - Defense Manager Daemon (DMD)
    - Application Transparent TLS (AT-TLS)
    - Intrusion Detection Services (IDS)

  - Policy-basierendes Routing (PBR)
  - Quality of Service (QoS)
  - TCP/IP-Profile-Konfiguration
  - Import existierender TCP/IP-Konfigurationen
  - Cloud Policy (Cloud)
- Bereitstellung einer Applikations-Setup-Task innerhalb des z/OSMF-Workflows
- Provisionierung von Netzressourcen mittels der IBM Cloud Provisioning and Management Services für z/OS.

Mit Hilfe einer grafischen Oberfläche werden die o. g. Policies angelegt, also die Zusammenstellung von Eigenschaften, Vorgaben und sonstigen Kriterien, nach denen bestimmte Verbindungen zu provisionieren, zu aktivieren und zu sichern sind. Alle Einstellungen, die über die Network Configuration Assistant Task innerhalb des z/OSMF vorgenommen werden, setzt der z/OS Communication Server Policy Agent in den IP-Stacks in Kraft (auch dynamisch).

Bei der Festlegung von kryptografischen Verfahren und Schlüssellängen für den Einsatz von Verschlüsselung (beispielsweise IPSec, TLS) sollte die Technische Richtlinie TR-02102 des BSI beachtet werden.

IBM zSystems Kryptographische Co-Prozessoren (Crypto Express Adapter) sind eine optionale und kostenpflichtige Erweiterung der jeweiligen IBM zSystems Server Generation. Crypto Express Adapter sind entwickelt worden, um die kryptographischen Fähigkeiten der CPACF Unterstützung zu erweitern, um weitere Algorithmen, Signatur- und Secure Key Verfahren für den noch besseren Schutz von transferierten und gespeicherten Daten zu unterstützen. Anwendungsbereiche sind unter anderem CCA-basierende Verfahren sowie PKCS#11-Signaturlösungen gemäß BSI TR-03111.

IBM z/OS Encryption Readiness Technology (zERT)

IBM z/OS Encryption Readiness Technology (zERT) ist Bestandteil vom z/OS Communication Server und wurde in mehreren Stufen bereitgestellt. Der zERT Network Analyzer, eine webbasierte grafische Benutzeroberfläche, hilft bei der schnellen Analyse von SMF-Daten, um die Sicherheitseigenschaften hinsichtlich Verschlüsselung von TCP und Enterprise Extender (EE) Verbindungen mit lokalen Endpunkten im z/OS-System zu analysieren. Die IBM zERT Network Analyzer Task kann auf zwei Wegen genutzt werden:

- über die traditionelle z/OSMF-Ansicht: Aufklappen der Analysis-Kategorie und Auswahl von IBM zERT Network Analyzer,
- über die z/OSMF-Desktop-Ansicht und Klick auf das Icon des IBM zERT Network Analyzers.

Der Analyzer dient der Kontrolle und dem Nachweis, ob und wie alle IP-basierenden Kommunikationen einer Authentisierung der Partner und dem Schutz der Session-Daten unterzogen werden. Datenbasis dafür sind zwei verschiedene SMF Records:

- SMF 119-11 „zERT Connection Detail" einmalig für jede Verbindung, geeignet für real-time Monitoring
- SMF 119-12 „zERT Summary" geschrieben durch die zERT „Aggregation"-Funktion, geeignet für historische Auswertungen.

Empfohlen wird, die IBM zERT Network Analyzer Task für folgende Funktionalitäten zu nutzen:

- Import von einem oder mehreren SMF Dump Datasets in die Datenbank des IBM zERT Network Analyzers. Die IBM zERT Network Analyzer Task inspiziert die SMF Records in den Datasets, extrahiert die Informationen aus den zERT Summary (type 119, subtype 12) SMF Records und bereitet die extrahierte SMF Information für jede Session auf. zERT Summary Records berichten pro Intervall die statistischen Daten und Verschlüsselungseigenschaften aller TCP- und EE-Verbindungen.

- Abfragen und Filterung der Session-Information in der IBM zERT Network Analyzer Datenbank nach Datum, Verbindung oder kryptografischen Eigenschaften.
- Ausführung von Abfragen und tabellarische Darstellung der Ergebnisse, anzeigbar auf Summary-Level oder detailliert pro ausgewählte Session.
- Wegschneiden unerwünschter Informationen aus der Datenbank des IBM zERT Network Analyzers.
- Exportieren der Ergebnisse von Abfragen in eine CSV-Datei (comma-separated values) für die Weiterverarbeitung in einer Tabellenkalkulation oder anderen Analysewerkzeugen.

Alle Einstellungen, die über die Network Configuration Assistant Task innerhalb des z/OSMF vorgenommen werden, setzt der z/OS Communication Server Policy Agent in den IP-Stacks in Kraft (auch dynamisch).

SYS.1.7.M12 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

SYS.1.7.M13 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

SYS.1.7.M14 Berichtswesen zum sicheren Betrieb von z/OS (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M15 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

SYS.1.7.M16 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

SYS.1.7.M17 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

SYS.1.7.M18 Rollenkonzept für z/OS-Systeme (S)

Übersicht über die RACF-Attribute SPECIAL, OPERATIONS, AUDITOR

Wie in SYS.1.7.M1 *Einsatz restriktiver z/OS-Kennungen* beschrieben, kann beispielsweise mit dem „Selected user attribute summary report“ des Data Security Monitor (DSMON) eine Auflistung aller Benutzenden erzeugt werden, die eines oder mehrere der o.a. Attribute auf System- oder auch Gruppenebene haben.

Es sollte sichergestellt werden, dass jedes Attribut mindestens an zwei verschiedene Benutzende (Stellvertretenden-Regelung) vergeben ist und einem Benutzenden nicht mehrere/alle Attribute zugeordnet sind. Es sollte immer geprüft werden, ob es statt der Verwendung der systemweiten Attribute ausreicht, ein Attribut nur auf Gruppenebene zu vergeben (group-SPECIAL, group-AUDITOR, group-OPERATIONS). Um die Verwendung des AUDITOR-Attributs einzuschränken, sollte die Verwendung von ROAUDIT (Read-Only Auditor) geprüft werden.

SYS.1.7.M19 Absicherung von z/OS-Transaktionsmonitoren (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M20 Stilllegung von z/OS-Systemen (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M21 Absicherung des Startvorgangs von z/OS-Systemen (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M22 Absicherung der Betriebsfunktionen von z/OS (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M23 Absicherung von z/VM (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M24 Datenträgerverwaltung unter z/OS-Systemen (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M25 Festlegung der Systemdimensionierung von z/OS (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M26 WorkLoad Management für z/OS-Systeme (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M27 Zeichensatzkonvertierung bei z/OS-Systemen (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M28 Lizenzschlüssel-Management für z/OS-Software (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M29 Absicherung von Unix System Services bei z/OS-Systemen (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M30 Absicherung der z/OS-Trace-Funktionen (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M31 Notfallvorsorge für z/OS-Systeme (S)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M32 Festlegung von Standards für z/OS-Systemdefinitionen (H)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M33 Trennung von Test- und Produktionssystemen unter z/OS (H)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M34 Batch-Job-Planung für z/OS-Systeme (H)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M35 Einsatz von RACF-Exits (H)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M36 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 möglichst über interne Kanäle erfolgen, d. h. entweder über

- Coupling Links
- HiperSockets
- virtuelle CTC-Verbindungen (Channel-to-Channel)
- shared OSA-Adapter
- Virtual Ethernet Port Isolation (z/VM VSWITCH für Gastsysteme)
- Shared Memory Communication
    - Remote Direct Memory Access (SMC-R)
    - Direct Memory Access over Internal Shared Memory (SMC-D)

oder eine Kombination aus obigen Mechanismen.

Die Vorteile einer solchen Konfiguration sind der Ausschluss von Risiken, die gegenüber LAN-Kommunikation existieren, sowie geringere Latenzzeiten.

Coupling Links werden verwendet, um z/OS LPARs mittels einer Coupling Facility (extern oder LPAR) zu einem Parallel Sysplex zu verbinden, auch über die Grenzen eines Z-Systems hinaus. Dafür werden spezielle I/O-Adapter benötigt, nämlich Coupling Express Long Range (LR) bzw. Integrated Coupling Adapter.

HiperSockets ermöglichen die Memory-to-Memory-Kommunikation zwischen LPARs eines Systems als virtuelle LAN-Verbindungen ohne die Notwendigkeit von I/O-Adaptern.

Für virtuelle CTC-Verbindungen müssen exklusiv den LPARs zugeordnete FICON-Ports zur Verfügung stehen und jeweils als CHPID-Typ CTC konfiguriert werden. Achtung: CHPID-Typ CTC wird im Dynamic Partition Manager (DPM) Modus nicht unterstützt.

OSA-Adapter können zwischen LPARs geteilt werden. Dies ermöglicht eine damit direkte Kommunikation ohne das Verlassen des IBM zSystems. In einigen Umgebungen ist es aber notwendig, den Netzverkehr und das Routing streng zu limitieren und zu kontrollieren. Die Maßnahmen dafür können unter Umständen vereinfacht werden, wenn über den Shared OSA-Adapter eine Port-Isolation und eine Routing-Kontrolle auf LPAR-Basis eingerichtet wird. Dafür müssen die LPARs in der OSA Access Table (OAT) registriert und ggf. isoliert definiert (ISOLATE=YES) werden.

Virtual Ethernet Port Isolation ermöglicht eine der beiden folgenden Funktionalitäten:

- Port Isolation, sie verhindert also die Kommunikation von Gastsystemen untereinander und erlaubt nur die Kommunikation von Gastsystemen mit Hosts oder Routern im externen Netz.

- Port Aggregation, sie erlaubt also die Bündelung von Kommunikation in ein externes Netz, die Isolation erfolgt durch Kombination von VSWITCH und OSA-Express.

Für Remote Direct Memory Access (SMC-R) werden spezielle I/O Adapter benötigt, nämlich 10/25 GbE RoCE (RDMA over Converged Ethernet). Der große Vorteil von SMC über RoCE ist das entfallene Routing und damit eine vereinfachte Konfiguration der Netzsicherheit (siehe auch SYS.1.7.M11 *Schutz der Session-Daten*).

Um den Zugriff auf Netzressourcen zu kontrollieren, wird die Einrichtung der entsprechenden Profile in der RACF-Klasse SERVAUTH empfohlen, auf die dann kontrolliert die notwendigen Berechtigungen erteilt werden können. Dafür gibt es eine Vielzahl von RACF-Profilen, unter anderem zur Berechtigung bzw. Kontrolle des Netzzugriffs in Bezug auf Kommunikationsrichtung (inbound, outbound, both) sowie benutzte IP-Stacks, Netze und Ports.

Welche Kombination von Profilen und Berechtigungen eingesetzt wird, ist von den jeweiligen Vorgaben abhängig. Empfohlen wird, zusätzlich zum Schutz der Ressourcen durch SERVAUTH-Profile spezielle Funktionen des IBM zSystems wie Intrusion Detection Services (IDS), syslogd-Isolation und IP-Filterung zu konfigurieren und zu aktivieren. Hinzu kommt die Kontrolle über die entsprechenden Kommandos zur Konfiguration, wie VARY TCPIP.

SYS.1.7.M37 Parallel Sysplex unter z/OS (H)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

SYS.1.7.M38 Einsatz des VTAM Session Management Exit unter z/OS (H)

Es sind hier noch keine Hinweise zur Umsetzung hinterlegt. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

3. Weiterführende Informationen

3.1. Wissenswertes

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

- APAR: Authorized Program Analysis Report
- CCA: Common Cryptographic Architecture
- CPACF: Central Processor Assist for Cryptographic Functions
- CPC: Central Processor Complex
- CTC: Channel-to-Channel-Verbindung
- DPM: Dynamic Partition Manager
- EIM: Enterprise Identity Mapping, Überführung einer Netz-ID in eine TSO-Kennung
- ETH: Ethernet
- FW: Firmware
- GA2: General Availability (generelle Verfügbarkeit) und Stufe (hier: 2)
- 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
- HW: Hardware

- ICSF: Integrated Cryptographic Service Facility (Bestandteil des z/OS)
- IETF: International Engineering Task Force
- IKE: Internet Key Exchange
- IPL: Initial Program Load, Startvorgang eines Betriebssystems
- IPSEC: Internet Protocol Security
- LIC: Licensed Internal Code
- LPAR: Logical Partition
- OAT: OSA Access Table
- PCHID: Physical Channel ID
- PSP: Preventive Service Planning
- RACF: Resource Access Control Facility, Werkzeug für Authentisierung, Autorisierung und Auditierung
- RoCE: RDMA over Converged Ethernet
- RSF: Remote Support Facility
- SE: Support Element, zur Konfiguration und Kontrolle des Systems
- SMF: System Management Facility, Werkzeug zur Ressourcen- und Systemüberwachung
- SMP/E: System Modification Program/Extended, Verfahren zur Software-Installation
- SVC: Supervisor Calls
- UACC: Universal Access Authority (RACF), Standard-Zugriffsberechtigung
- zACS: z/OS Authorized Code Scanner
- zFS: zSeries File System, Dateisystem, das unter z/OS und Unix System Services (USS) eingesetzt wird
- z/OSMF: z/OS Management Facility, Oberfläche für die Administration des z/OS

3.2. Quellenverweise

Der Hersteller IBM gibt weitere Informationen zum Thema IBM zSystems Plattform Security über folgende Quellen:
https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity (Integrity Statement)

https://www.redbooks.ibm.com (IBM Redbooks)
SG24-8410-01: Getting Started with z/OS Data Set Encryption
SG24-8472-01: IBM Security Guardium Key Lifecycle Manager
SG24-8455-00: IBM Fibre Channel Endpoint Security for IBM DS8900F and IBM Z
SG24-8457-00: Getting started with z/OS Container Extensions and Docker

https://www-01.ibm.com/servers/resourcelink (Ressourcelink)
(Installierte zSystems-Generation bzw. TKE-Version auswählen.)

SC28-7027-00: z16 HMC Security
GC28-6980-03: IBM Z Service Guide for Trusted Key Entry Workstations
SC14-7511-10: TKE Workstation User's Guide TKE Version 10.0

https://www.ibm.com/docs/en/zos (Dokumentation)

https://www.ibm.com/docs/en/SSLTBW_2.5.0 (aktuell z/OS V.2.5)
SA23-2289-50: z/OS Security Server RACF Security Administrator's Guide

SA23-2290-50: z/OS Security Server RACF Auditor's Guide
SA32-0991-50: z/OS JES2 Initialization and Tuning Guide
SA38-0667-50: z/OS MVS System Management Facilities (SMF)
SC27-8419-50: IBM z/OS Management Facility Configuration Guide
SC27-8420-50: IBM z/OS Management Facility Programming Guide
SC23-6843-50: IBM Health Checker for z/OS User's Guide
GA32-0891-50: z/OS Planning for Multilevel Security and the Common Criteria
SC28-3123-50: IBM z/OS Authorized Code Scanner Guide
SA23-2229-30: Encryption Facility for z/OS Planning and Customizing
SA23-2230-30: Encryption Facility for z/OS Using Encryption Facility for OpenPGP
SC23-6788-50: z/OS IBM Tivoli Directory Server Administration and Use for z/OS
SC27-4942-50: z/OS SDSF Security Migration Guide
SC27-3650-50: z/OS Communications Server: IP Configuration Guide
SC14-7505-08: z/OS Cryptographic Services Integrated Cryptographic Service Facility Overview
SA23-2286-50: z/OS Cryptographic Services PKI Services Guide and Reference
SA23-2297-50: z/OS Integrated Security Services EIM Guide and Reference
SC23-6786-50: z/OS Integrated Security Services Network Authentication Service Administration
SA38-0680-50: z/OS Unicode Services User's Guide and Reference
SC27-6806-50: z/OS OpenSSH User's Guide

Dringend empfohlen wird die Registrierung und automatische Information im „IBM Z and LinuxONE Security Portal" für Security Alerts und entsprechende MCL und Software Fixes auf der folgenden Webseite:

https://www-03.ibm.com/systems/campaignmail/z/capabilities/system-integrity/register-zsecurity-portal