fit for mainframe

„Certified IBM Mainframe Security Professional” für

- **Systemprogrammierer**
- **systemorientierte Mitarbeiter**
- **künftige Security Administratoren**

Version 2.1 vom 4. Februar 2018

Autor: Wolfram Greis
wolfram.greis@mainframe-academy.eu

European Mainframe Academy GmbH
Am Klostergarten 3
D 78337 Öhningen
Tel. +41-79-340 64 52
info@mainframe-academy.de

European Mainframe Academy AG
Obergass 23
CH 8260 Stein am Rhein
Tel. +41-52-558 20 40
wolfram.greis@mainframe-academy.eu

© 2008-2014 European Mainframe Academy, Augsburg/Stein am Rhein

Inhaltsverzeichnis

© 2008-2018 European Mainframe Academy, Augsburg/Stein am Rhein

1 Ziele des Ausbildungsmoduls

2 Informationen zum "Blended Learning" der EMA

Die Lehrgangsmodule der EMA sind eingeteilt in Pflichtstoff und Wahlstoff. Der Pflichtstoff ist prüfungsrelevant, d.h., dass die entsprechend vermittelten Kenntnisse in Tests, Prüfungen und praktischen Arbeiten vorhanden sein müssen und abgefragt werden, falls am Ende des Moduls ein Zertifikat erlangt werden soll.

Der Wahlstoff kann auf freiwilliger Basis durchgearbeitet werden. Selbstverständlich stehen für sämtliche Belange qualifizierte Fachkräfte für die Beantwortung von Fragen zur Verfügung.

Der durchschnittliche Lernaufwand für den Pflichtstoff beträgt ca. 10 Stunden pro Woche.

Die Module bestehen aus:

- Präsenzveranstaltungen (Kick-off und Abschluss)
- Virtuelle Klassenzimmer
- E-Learning
- Theoretische und praktische Übungen

3 Kosten

Die Kosten für dieses Modul betragen € 6‘400 / CHF 7‘500 zzgl. gesetzl. MWSt.

Bei mehr als einem Teilnehmer aus demselben Unternehmen gewähren wir eine äusserst interessante Rabattierung!

4 Inhaltsbeschreibung

Im Folgenden werden die Module detailliert beschrieben. Die Zahl in Klammern bei den Inhalten gibt die geschätzte durchschnittliche Bearbeitungszeit in Stunden an.

© 2008-2018 European Mainframe Academy, Augsburg/Stein am Rhein

4.1 Kick-off Workshop (1,5 Tage)

Präsenzworkshop
Mit diesem eintägigen Workshop wird die Basis einer erfolgreichen Zusammenarbeit während der gesamten Lernphase gelegt. Der Workshop findet je nach Teilnehmerherkunft in Deutschland, Schweiz oder Österreich statt.

Dauer **1,5 Tage**

Datum **Nächster Termin: 22.-23. März 2018**

Ort **Augsburg**

Ziele des Workshops

Mit diesem Präsenzworkshop sollen drei Dinge erreicht werden:

- Die Teilnehmer und die Key-Dozenten lernen sich gegenseitig kennen
- Die Teilnehmer lernen die wichtigsten E-Learning Werkzeuge kennen, vor allem das Virtuelle Klassenzimmer
- Die Teilnehmer bekommen einen ersten Überblick über die Seminarinhalte

Inhalt

Einführung
Vorstellungsrunde
Einführung in das Thema

Lerneffizienz
Lernen und Erkenntnisse der Neurobiologie
Effizientes Lernen

E-Learning & Blended Learning
Der Bedeutung von E-Learning
Die Vorteile des Blended Learning
Integration von Web 2.0
E-Learning Werkzeuge im Überblick

Lernplattform Moodle
Übersicht über die Lernplattform
Aufbau der Lernplattform

Das Virtuelle Klassenzimmer
Ziele einer VC-Session
Unterschiede zum herkömmlichen Klassenzimmer
Einsatz des Virtuellen Klassenzimmers

Zugriff auf den Mainframe
Die Infrastruktur der EMA
Zugriff auf den IBM Rechner

Security Einführung
Anforderungen
Verschlüsselungstechniken
Stand der Technik
Gesamtüberblick über das Lernmodul

Security und Mainframes (Überblick)
Anforderungen an die Security
Worin unterscheidet sich Mainframe-Security von andern Plattformen?
z/OS und z/OS UNIX System Services
Die Rolle des z/OS Security Servers
Gruppenarbeit

© 2008-2018 European Mainframe Academy, Augsburg/Stein am Rhein

4.2 z/OS Security Server Basics (ca. 40 Stunden)

Ziele dieses Untermoduls
Die Teilnehmer kennen den z/OS Security Server und insbesondere RACF. Sie können die diversen Profilarten von RACF beschreiben. Sie kennen die Befehle, um Profile einzurichten und zu verändern. Sie können abschätzen, wann welche Befehle sinnvoller Weise unter TSO/ISPF und wann als Batchjob abgesetzt werden.

Inhalt

RACF Überblick
Anforderungen an ein Security System
Sicherheit im Rechenzentrum
Physische Sicherheit
Sicherheit des Betriebssystems
RACF als Baustein eines Geamtkonzepts
RACF Funktionsüberblick
RACF Profilarten
System Access Facility (SAF) und RACF

RACF Aufbau
Hierarchische Architektur
Gruppenkonzept
RACF Konzept & Konventionen
Generic Profiles
Schutz von Dateien
Schutz von General Resources

Komponenten von RACF
RACF Datenbank
RACF Befehle
Verwaltung mit Batchjobs
ISPF Schnittstelle

Reporting und Utilities
RACF und SMF
RACF Utilities
RACF Audit Funktionen

RACF Optionen

Verwaltung von RACF Benutzern

© 2008-2014 European Mainframe Academy, Augsburg/Stein am Rhein

4.3 z/OS Security Server Vertiefung (ca. 40 Stunden)

Ziele dieses Untermoduls
Die Teilnehmer kennen erweiterte Möglichkeiten von RACF. Sie können z/OS Subsysteme wie DB2, CICS und weitere z/OS Komponenten aus Security-Sicht verwalten.

Inhalt

Erstellen und Migrieren einer RACF Datenbank

Schutz von JES uns Spool-Ressourcen

Schutz von SDSF

Schutz von VTAM Ressourcen

RACF in einer Sysplex-Umgebung

RACF und UNIX System Services
UID und GID Verwaltung
Schutz von Prozessen
Webserver Security

Security Labels

z/OS HTTP Server Security

RACF und WebSphere Application Server

RACF und WebSphere MQ

RACF und Password Synchronization

RCAF Macros und Schnittstellen

© 2008-2014 European Mainframe Academy, Augsburg/Stein am Rhein

4.4 Verschlüsselungstechniken (ca. 40 Stunden)

Ziele dieses Untermoduls
Die Teilnehmer kennen die Verschlüsselungstechniken und deren historische Entwicklung bis in das Computer- und Internet-Zeitalter. Sie kennen den Unterschied zwischen symmetrischen und asymmetrischen Techniken sowie deren Vor- und Nachteile. Sie können die Unterschiede zwischen DES, RSA und AES erklären.

Inhalt

Historie der Verschlüsselung von Informationen
Mesopotamische Tontafel
Caesar`s Verschiebealgorithmus

Kryptologie / Kryptographie / Kryptoanalyse
Terminologie und Begriffe
Kryptografische Algorithmen
Kryptografische Protokolle
(Private Key / Public Key Verfahren)
Sicherheit von Schlüsseln

Arten von Chiffren
Klassische Chiffren
Blockchiffren (DES, AES)
Public-Key-Kryptographie

Authentifikation und digitale Signatur
Einwegfunktionen
Zero-Knowledge-Protokolle
Digitale Signaturen

Public Key Kryptographie
RSA Algorithmus und Implementierung
Algorithmen und Elliptische Kurven

Public Key Infrastruktur (PKI)
Prüfung öffentlicher Schlüssel
Trustcenter (CAs)
Zertifikatshierarchie
Web-of-Trust

Public Key Systeme
Pretty Good Privacy (PGP)
S/MIME und das X.509 Protokoll
Secure Shell (SSH)
SSL und TLS
IP Security und VPN

Elektronische Systeme
Elektronisches Bargeld
Elektronische Zahlungssysteme

Gesetzliche Rahmenbedingungen
Deutsche und Europäische Regelungen
US Exportgesetze

© 2008-2014 European Mainframe Academy, Augsburg/Stein am Rhein

4.5 System z Hardware Kryptographie (40 Stunden)

Ziele dieses Untermoduls
Die Teilnehmer kennen die kryptographischen Möglichkeiten, die in der IBM Hardware z10, 196, z114 und zEC12 eingebaut sind und wie diese mit der ICSF (Integrated Cryptographic Service Facility) Komponente des z/OS zusammenarbeiten.

Sie kennen die zur Verfügung stehenden APIs und dien Interaktionen mit dem z/OS Security Server (RACF) und die Schlüsselverwaltung.

Ebenfalls behandelt werden die Möglichkeiten in Verbindung mit Trusted Key Entries (TKE) und das Distributed Key Management System (DKMS).

Inhalt

Integrated Cryptographic Service Facility
Infrastruktur und Implementation
IBM CCA (Common Cryptographic Architecture) API
Key Management mit ICSF

Performance Considerations

Augmented SAF/RACF Protection

ICSF Installation & Customization
Installation von ICSF
Anpassung an die eigene Umgebung
ICSF Administration

Die optionale TKE Workstation

Die optionale DKMS Workstation

© 2008-2018 European Mainframe Academy, Augsburg/Stein am Rhein

4.6 Abschlussworkshop (1 Tag)

Präsenzworkshop
Mit diesem eintägigen Workshop werden die Ergebnisse zusammengefasst und offene Fragen beantwortet.

Dauer **1 Tag**

Datum **Nächster Termin: TBA**

Ort **TBD**

Ziele des Workshops

- Die wichtigsten Themen und Schwerpunkte werden noch einmal zusammengefasst
- Die Teilnehmer beantworten Verständnisfragen der Coaches / Referenten um den Wissenstransfer sicher zu stellen.
- Die Teilnehmer stellen Fragen, die sich während der Ausbildung ergeben haben.
- Prüfungsarbeit zur Erlangung des Zertifikats "**Certified Mainframe Security Professional**"

© 2008-2018 European Mainframe Academy, Augsburg/Stein am Rhein