



openHPI Security Grundlagen

Wolfram Greis
European Mainframe Academy
Stein am Rhein (CH)

- Unternehmensdaten sind heute in der Regel das wichtigste Gut einer Firma.
- Daten und Programme müssen gegen unberechtigte Zugriffe geschützt werden.
- Dies betrifft sowohl den Schutz vor externen Personen (Kunden, Geschäftspartner, Hacker etc.) als auch vor internen Personen.
- Das Verständnis für wirksame Sicherheitsfunktionen in Verbindung mit dem Betriebssystem z/OS ist in diesem Zusammenhang wichtig sowie auch die Kenntnis über die entsprechende Implementation.

- Im Laufe der Zeit wurde es immer einfacher, auf Rechnern gespeicherte Informationen zu erstellen und darauf zuzugreifen.
- Während es in früheren Zeiten noch einer Handvoll hoch spezialisierter Experten möglich war (Closed Shop Betrieb), auf kritische Daten zuzugreifen, ist dies heute grundsätzlich vielen Personen möglich, häufig sogar über eine Internet-Verbindung.
- Umso wichtiger ist heute der Schutz der Daten vor unberechtigten Zugriffen.
- Zugriffskontrolle umfasst die Methoden, entsprechende Berechtigungen und Zugriffe auf Ressourcen zu gewähren oder einzuschränken.
- Es handelt sich hierbei um eine logische Zugriffskontrolle.
- Diese logische Zugriffskontrollen werden i.d.R. in das Betriebssystem integriert und werden häufig durch Zusatzwerkzeuge ergänzt.

- **Physische Sicherheit**
 - Zutrittskontrolle
 - Backup/Katastrophenplan
- **Sicherheit des MVS**
 - Systemintegrität
 - Autorisierte Programme
 - Program Property Table (PPT)
 - Konsolprotokoll
 - System Management Facility (SMF)
 - Kryptographie (Verschlüsselung)
 - Resource Access Control Facility (RACF)



- Resource Access Control Facility (RACF)
- DCE Security Server
- z/OS Firewall Technologien
- Lightweight Directory Access Protocol (LDAP) Server
- Open Cryptographic Enhanced Plugin (OCEP)

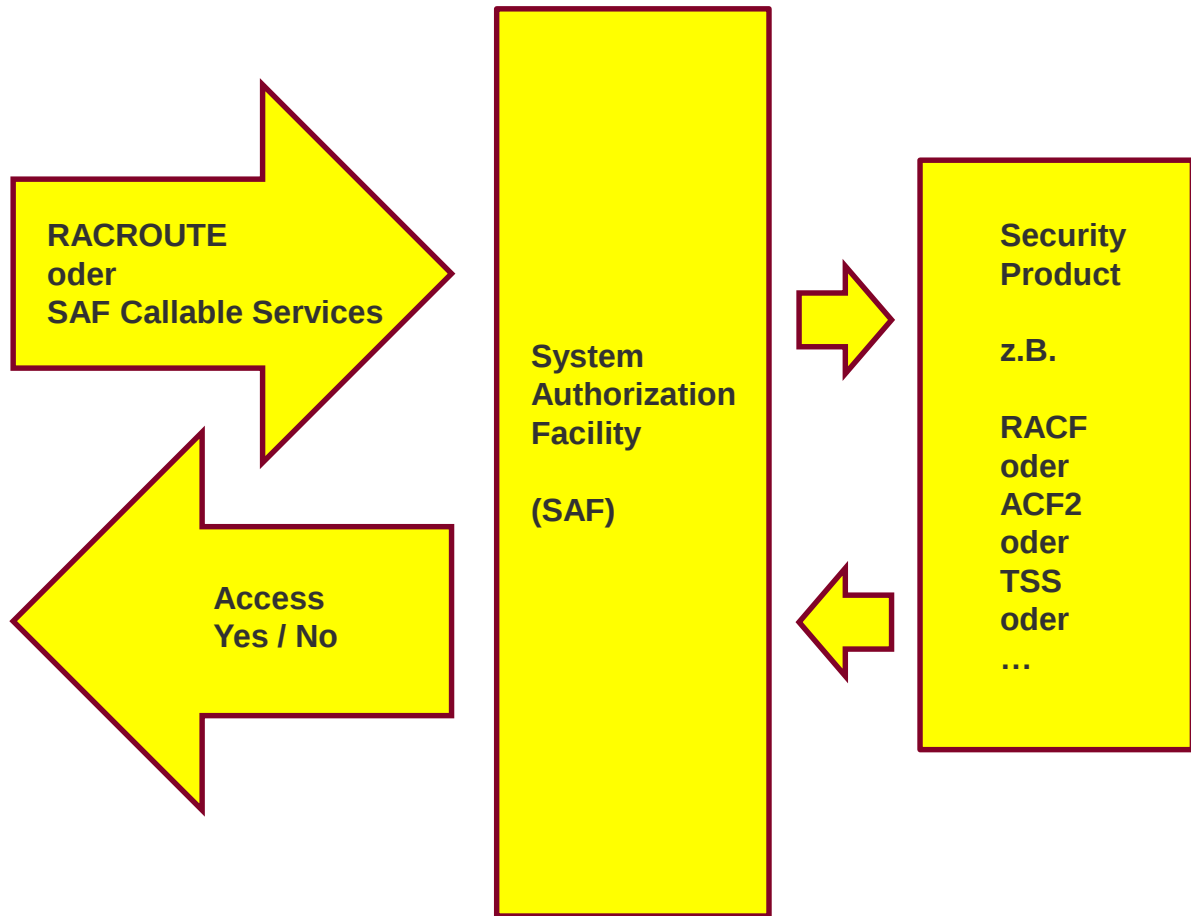
- Identifikation von Benutzern
 - Jeder Benutzer sollte seine eigene Kennung haben
 - Eigenverantwortlichkeit
- Verifizierung
 - Durch ein Passwort muss geprüft werden können, ob der Benutzer die Person ist, für die sie sich ausgibt
- Zugriffskontrolle
 - Geschützte Ressourcen dürfen nur von berechtigten Personen benutzt werden.
- Kontrolle und Protokollierung
 - Es muss eine einfache Möglichkeit der Überwachung geben
 - Ereignisse müssen protokolliert werden können
- Benutzerschnittstelle
 - Klare Strukturen
 - Einfache Handhabung

SYSTEM AUTHORIZATION FACILITY

Ressource Manager nutzen SAF
Interfaces oder RACROUTE

Ressource Manager sind z.B.:

- DFP (OPEN,SCRATCH ...)
- USS
- VSAM / AMS
- DFSMS
- CICS
- DB2
- IMS
- TSO
- JES
- SDSF
- WebSphere
- MQ
- etc.



Fragen / Diskussionen
gerne im Forum zu diesem MOOC