

Thoughts Concerning How Secure Is Your System?

Ingenieurbüro Jörg Grössler
IJG, Berlin

WHAT DATA SECURITY MEANS

- To be able to rebuild the file system in case of a disaster
- To restrict access on various type of data.

STANDARD FILE BACKUP FACILITIES IN MPE

- Sysdump, Reload (based on magnetic tape)
- Store, Restore (tapes)
- User Logging (based on disc or tape)
- Private volumes (disc)

PROBLEMS WITH STANDARD FILE BACKUP

- Tape read error during RELOAD
 - system cannot be started
 - next action "must be RELOAD"measures:
 - change disc packs before RELOAD
 - RELOAD with "ACCOUNTS-only" then RESTORE the remaining files (very time consuming)
- Tape read error during RESTORE
 - all files stored behind error point cannot be re-storedmeasure:
 - use RESTORE or GETFILE2 program
- User logging causes system overheadmeasure:
 - consider special logging during program design

PROSPECTS FOR TAPE-BACKUP SYSTEM

- GETFILE-facility will be improved
- Special STORE-RESTORE system is considered (this possibility includes features like UPDATE and APPEND)

RESTRICTIONS IN DATA ACCESS

- Account-system (users, groups, accounts with different passwords)
- User capabilities (SM, PM, PH, etc.)
- Filenames with passwords
- Privileged files
- File access capabilities on user/group- and file-level
- RELEASE/SECURE-commands

SEVEN POSSIBLE WAYS TO CRACK THE SYSTEM

1. FIELD.SUPPORT

measure:

Password on SUPPORT-account

Or remove SUPPORT-account from the system.

2. Jobs in PUB.SYS-group

measure:

Password on job-file or

Put job into other SYS-group.

3. LISTUSER@.@;LP

measure:

Log-on-UDC or perform command

Not in PUB.SYS-group.

4. Open all files of the system

measure:

Special analysis of system logging

5. Read terminal buffers (PM-capability needed)

measure:

Remove PM-capability

6. Reading tapes

measure:

Keep track of all tape-transactions also using system logging

7. FOPEN on terminals

measure: ??

8. . . .

