3CAT™
jason.viola@3cat.net

3CAT

SAP Security

Jason Viola CISA

3CAT™
jason.viola@3cat.net

Scope

- What is SAP R/3
- Overall architecture
- Some potential security exposures
- Management controls
- Some useful SAP transactions and reports
- An overview of SAP audit tools

3CAT™
jason.viola@3cat.net

What is SAP R/3

- SAP is the largest enterprise software company
- SAP is the fourth largest software company
- SAP's core concept 'organisational integration'
- The Runtime system 3 (SAP R/3)
- SAP Industry Solutions

3CAT™
jason.viola@3cat.net

Overall architecture

- Database servers
- Application servers
- Presentation
- + Infrastructure

3CAT™
jason.viola@3cat.net

Security exposures

- Database servers
  - ADABAS D - Unix or Windows
  - DB2 - AIX, DB2/400 - OS/400 ... and more
  - Informix - Unix
  - MS SQL - Windows
  - Oracle - Unix or Windows

3CAT™
jason.viola@3cat.net

Security exposures

- Database servers
  - SAP default accounts
    - SAPR3 - sapr3
    - OPS$<name of instance>adm - no password
  - Oracle
    - SYS - “change_on_install”
    - SYSTEM - “manager”
    - <ORACLE SID>ADM - UNIX account that owns SAP directories

3CAT™
jason.viola@3cat.net

Security exposures

- Application Layer
  - Some default accounts
    - SAP* - "06071992" - after deletion "pass"
    - DDIC - "19920706"
    - SAPCPIC - "admin"
    - EARLYWATCH - "support" - read access
- ABAP - Migration access
- BAPIs - Check logon ID security
- Table Logging - rec/clients = ALL

3CAT™
jason.viola@3cat.net

Security exposures

- Application layer
  - Reports that should be restricted
    - RDDPWCHK - Bypasses invalid login attempt #
    - RSDELSAP - Can delete the SAP* account
    - SRCDOK99 - Can delete change documents
    - RSTBPDEL - Can delete table change logs
    - RS3URETE - Can change ABAP without Dev Key
  - Access authorisation objects must not be disabled

3CAT™
jason.viola@3cat.net

Management controls

- Audit's role
- Information Security involvement
- An SAP security configuration check list

jason.viola@3cat.net

Management controls

- Co-ordination of SAP Projects (ASAP?)
- Project Manager's security responsibility
- Operations hand-over quality assessment

3CAT™
jason.viola@3cat.net

Management controls

- SAP Authorisation Concept
  - Complexity, scale, diversity
  - Only 217 authorisations in basis
  - 1200 authorisations in HR, FI & Logistics
  - Roles and Profiles only
  - Soon... Only Roles
  - Regular re-certification

3CAT™
jason.viola@3cat.net

Discovering exposures

- Review the architecture
- Security Testing
- Find accounts with default passwords
  - Run report RSUSR003 - cross-client check
- Confirm who can run what reports
  - Run transactions sa38, sc38 and se38
- Confirm which tables are being logged
  - Run report RSTBHIST

jason.viola@3cat.net

Discovering exposures

- Check the transport directory
  - Use transaction rz10 Look for DIR_TRANS
- There are more... Many more

jason.viola@3cat.net

SAP audit tools

- Licences can be purchased for
  - Admin Tool
  - bv Control
  - CheckAud
- Weese - Weese consultants use only
- In addition, some of the accountancy firms have their own software, for their Consultants use only

3CAT™
jason.viola@3cat.net

3CAT

SAP Security

ANY QUESTIONS?

Jason Viola CISA