PeopleSoft Security

Real-World PeopleSoft Vulnerabilities: A “Most Wanted” List

System Efficiency
Ben Klang

Agenda

- The What and the Why:
  - How this presentation was created
- System Efficiency's Most Wanted
- What They Are:
  - The Most Wanted Exposed
- Final Thoughts
- Questions

Real-World Vulnerabilities

- This information has been collected based on the experiences of System Efficiency Consultants in the field
- Don't laugh: The problems found here have been found in the wild (tsk tsk)
- The problems and solutions presented here will make you provably more secure
- Do this before you buy your fancy software/hardware/expensive bandaid

Why You Care

- 2007 Average Annual Loss was $350,424
  - more than double that of 2006
- Reverses a five-year downward trend
- It's not just random:
  - nearly 1 in 5 incidents reported for 2007 were targeted attacks
- Financial Fraud overtakes Virus as number 1 reported incident

Source: 2007 Computer Security Institute Survey

System Efficiency's Most Wanted

- Default User Accounts
- Weak Node Passwords
- Shared Accounts
- “Most Privilege” Security Model
- Process Blindness
- Policy Amnesia

Default User Accounts

- WebLogic or WebSphere Admin
  - WebLogic: “system”
  - Tuxedo: “tpsysadm”
- Oracle
  - “sysdba”
  - “internal”
- PeopleTools: VP1 and Friends
- Default account access can be mitigated at other levels such as firewalls and OS controls

Weak Node Passwords

- PeopleSoft Nodes are the gates to the kingdom
- Nodes should be secured separately in Dev, QA and Production
- Node security may rely on:
  - Password
  - X.509 Certificate
- Demo

Shared Accounts

- “Who made that entry?”
- Access revocation nightmare
- Audit impossibility
- Often stems from a lack of clearly defined process

"Most Privilege" Security Model

- The opposite of "Least Privilege"
- Unrestricted use of "?Admin?" role
- Filesystem Permissions ("chmod 777")
- Everyone knows the "root" password
- Often the result of "thrashing," or frantic attempts to "just make it work"
- "We'll clean it up later" - No, You Won't.

Process Blindness

- Defined as a pervasive ignorance of how the "big picture" fits together
- What needs to be audited?
- Why?
- False security may be worse than no security

Policy Amnesia

- Policy Manuals are not NYT Best Sellers
- Staff evolution and turnover lead to awareness gaps
- “I've always done it this way”
- Must explain the “Why” as well, not just the “What”

Conclusion

- If it hasn't happened to you yet, it will
- Be concerned about what you do not know
- Security is a mind-set
  - Requires Policy definition and enforcement
  - NOT just a technology problem
  - Must have buy-in from all levels within the organization
- Some basic consideration goes a long way

Questions?