



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Computer disaster scenarios:
 - Virus infection (perhaps on every NT node)
 - Physical/hardware failure
 - Malicious hacking
- Disaster plan requirements:
 - Continue data-taking as long as possible
 - Quick recovery, even over all NT nodes
 - Easy maintenance



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Current backup scheme:
 - Retrospect Server Backup machine on offline subnet and Retrospect Clients on each online subnet NT node
 - “SnapShot” (catalog) resides on Backup machine for each online node
 - “Backup set” (file archive) resides on CD-RWs (one or more) for each online node:
 - 1st week: Full backup “A set”
 - 2nd week: Full backup “B set”
 - 3rd week: Normal (incremental from full) “A set”
 - 4th week: Normal “B set”
 - 5th week: Normal “A set” (again incremental from 1st week)
 - 6th week: Normal “B set”
 - Up to 12 weeks
 - CD-RWs written on 10 CD-RW drives; organizational headache storage & labeling



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Current backup scheme (continued)
 - Each primary user of each NT node produced list of folders to be backed up
 - Disaster recovery (disregarding security issues):
 - Reformat hard drive
 - Install Windows NT
 - Install iFIX/DMACS software
 - Restore backup folders
 - Worry about updates and patches to system, iFIX, drivers, etc. that did not get installed
 - Security issues:
 - How to prevent reinfection while recovering
 - Updates and patches most easily available over network
 - Maintaining history of patches for quick recovery difficult, especially with remote institutions



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Proposed new backup scheme:
 - Backup to new 9.5 GB DVD-RAM drives (4 drives for nightly rotation through 22 nodes once per week)
 - Size sufficient to put all “backup sets” (full and incremental) for 12 week period on one DVD-RAM
 - Use “A set” first 12 weeks, then “B set” next 12 weeks for 6 months of archiving (recycle if costs remain high)
 - Reduces 100s of CD-RWs to 44 DVD-RAMs
 - Retrospect has DVD-RAM drivers already built-in
 - “SnapShots” can be rebuilt from “backup sets” if Backup machine compromised



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Proposed new backup scheme (continued):
 - Backup only entire system disk (C: drive)
 - Require users to put all current files necessary to run critical system and only these files on C: drive:
 - Windows NT
 - iFIX/DMACS software
 - Program executables (**not** object files or source code)
 - iFIX local database
 - Support files and programs
 - Latest patches and bug fixes
 - With Retrospect wizard (?), restore entire C: drive image to working order
 - Pro: Quick, order of 1 hour
 - Con: Can only restore one machine at a time



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Disaster recovery scenario:
 - Virus infection or malicious attack detected
 - Presumably, hardware damage does not require network disconnect
 - Online subnets (236, 237) disconnected; data-taking continues till convenient time (end of shot?)
 - Cannot start recovery without go-ahead from CD, and Norton patch to virus detection (if virus infection)
 - Backup machine (on offline net) checked for infection; if found, first must remove from network and restore
 - All compromised machines on online subnet wiped clean
 - Backup machine connected to online subnet with reserved IP address



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

- Disaster recovery scenario (continued):
 - Restore one NT node C: drive at a time
 - Restore via Retrospect disaster recovery preparation wizard (?)
 - Check again for virus infection
 - If found, start over with earlier “backup set”
 - As NT nodes are restored, can immediately start running critical systems (?)



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

● Implementation:

- Investigating DVD-RAM drives now, will buy one soon for test
- If test is successful, move to buy three more (typically 3-4 machines per day are backed up in weekly rotation)
- Media more expensive: \$50/9.5 GB for DVD-RAM vs. <\$1/0.65 GB for CD-RW
- Test restoration on CDFS3 when new machine is built
- Train more people to do disaster recovery



Computer Security— Windows NT Disaster Recovery

Steve Hahn
Disaster Recovery
10/11/2001

● Unresolved Issues:

- How exactly does restoration work?
- How do other (non-critical) portions of NT nodes get backed up and restored in this scenario?
 - Currently, each user is doing backups on their own machines in their own fashion