

Principper for Sys Adm 2

sw6 torsdag 7/4-05

agenda

- Debugging – Fix It once
- Security
- Beredskab
- Etik mm

Debugging – forstå problemet

- Forstå problemet
 - Hvad forventer vi sker ?
 - Hvad sker der rent faktisk ?
 - Hvad præcis prøver brugeren at gøre ?
 - Vidende brugere
 - tag ikke deres analyse for pålydende – check selv
 - gælder også når vi selv er brugeren – det er sikkert ...

Debugging – Find årsagen

- Opstil en hypotese
- Test den
- Elimination / Refinement
 - til problemet forsvinder / opstår
- Systematik
 - Hvad var den seneste ændring
 - kan være en genvej ... men f.eks hw fejl opstår ...

Debugging – Fix It Once !

- Lav en ændring der løser problemet ved roden
 - ”behandl årsagen ikke symptomet”
- Er det nødvendigt med et hurtigt fix så ...
 - Besked til mig selv : ”Fix det her permanent”
 - Mail – Helpdesk system eller lignende
 - ”mail fra kommandolinien er en god ting”

IT - sikkerhed

- ”IT-sikkerhed er primært en management opgave”
 - ikke gjort med teknik alene !
 - Kræver opbakning fra såvel ledelse som brugere
 - bør være centralt styret
 - ensartede politikker
 - ledelses opbakning / funktion

Opgaven – IT sikkerhedssystemer

- Tillad brugeren at arbejde effektivt
- Opretholder en fornuftig grad af sikkerhed
- Simpelt – er godt
- kan implementeres med rimelig tid / ressource forbrug

Hvad beskytter vi

- information i virksomheden
- integritet / fortrolighed af data
 - backup
 - adgangskontrol
 - også fysisk !
 - procedurer , revision
- tilgængelighed af resourcer
 - drift , hardware,

Sikkerhedspolitik

- Acceptable Use
- Overvågning og privacy
- Forbindelse til Nettet
 - samarbejdspartneres sikkerhed !
- Data og log arkiverings policy
 - = backup
 - lovgivning
- Og mere ...
 - DS 484 , best practices , lovgivning

Følg med

- Computer Emergency Response Team
 - www.cert.dk , www.cert.org
- www.sans.org
- BugTraq
 - www.securityfocus.com
- NTBugtraq
 - www.ntbugtraq.com
- seclists.org



Incident Response

Chapter 10

Panko, Corporate Computer and Network
Security

Copyright 2004 Prentice-Hall

Incident Response

- Incidents Happen
 - Protections sometimes break down
- Incident Severity
 - False alarms
 - Minor incidents
 - Major incidents
 - Disasters

Incident Response

- Speed is of the Essence
 - Attackers must be stopped quickly to minimize damage
 - The need for prior preparation for speed and correctness during incidents
 - Most important actions occur before the incident happens
 - Backup, training, rehearsals, etc.

Intrusion Response

- Initiation and Analysis
 - Initiation
 - Report a potential incident
 - Everyone must know how to report incidents
 - Analysis
 - Confirm that the incident is real
 - Determine its scope: Who is attacking; what are they doing

Intrusion Response

- Containment
 - Disconnection of the system from the site network or the site network from the internet (damaging)
 - Harmful, so must be done only with proper authorization
 - Black-holing the attacker (only works for a short time)
 - Sometimes, continue to collect data (allows harm to continue) to understand the situation better

Intrusion Response

- Recovery
 - Repair of running system (hard to do but keeps system operating with no data loss)
 - Restoration from backup tapes (loses data since last backup)
 - Reinstallation of operating system and applications
 - Must have good configuration documentation before the incident

Intrusion Response

- Punishment
 - Punishing employees is fairly easy given employment laws, unless the firm is unionized
 - Pursue prosecution?
 - Cost and effort
 - Probable success if pursue (often attackers are minor)
 - Loss of reputation

Intrusion Response

- Punishment
 - Collecting and managing evidence
 - Call the authorities for help
 - Preserving evidence (the computer's state changes rapidly)
 - Information on disk: Do immediate backup using forensics disk copier only
 - Ephemeral information: Stored in RAM (who is logged in, etc.)

Intrusion Response

- Punishment
 - Collecting and managing evidence
 - Protecting evidence and documenting the chain of custody
 - Ask upstream ISPs for a “trap and trace” to identify the attacker
- Post-Mortem
 - After the incident, reflect on what you learned and change your intrusion response method accordingly

Intrusion Response

- Communication
 - Warn affected people: Other departments, customers
 - Might need to communicate with the media; Only do so via public relations

Intrusion Response

- Protecting the System After the Attack
 - Hacked system must be hardened
 - Especially important because many hackers will attack it in following weeks or months

Business Continuity Planning

- Business Continuity Planning
 - A business continuity plan specifies how a company plans to restore core business operations when disasters occur

Business Continuity Planning

- Business Process Analysis
 - Identification of business processes and their interrelationships
 - Prioritizations of business processes
 - Downtime tolerance (in the extreme, mean time to belly-up)
 - Resource needs (must be shifted during crises)

Business Continuity Planning

- Communicating, Testing, and Updating the Plan
 - Testing (usually through walkthroughs) needed to find weaknesses
 - Updated frequently because business conditions change and businesses reorganize constantly
 - Telephone numbers, e-mail addresses, etc. must be updated even more frequently than the plan as a whole

Disaster Recovery

- Business Continuity Planning
 - A business continuity plan specifies how a company plans to restore core business operations when disasters occur
- Disaster Recovery
 - Disaster recovery looks specifically at the technical aspects of how a company can get back into operation using backup facilities

Disaster Recovery

- Types of Backup Facilities
 - Hot sites
 - Ready to run (power, HVAC, computers): Just add data
 - Considerations: Rapid readiness versus high cost

Disaster Recovery

- Types of Backup Facilities
 - Cold sites
 - Building facilities, power, HVAC, communication to outside world only
 - No computer equipment
 - Might require too long to get operating

Disaster Recovery

- Types of Backup Facilities
 - Site sharing
 - Site sharing across firms (potential problem of prioritization, sensitive actions)
 - Site sharing with a firm's sites (problem of equipment compatibility and data synchronization)

Disaster Recovery

- Types of Backup Facilities
 - Hosting
 - Hosting company runs production server at its site
 - Will continue production server operation if user firm's site fails
 - If hosting site goes down, there have to be contingencies

Disaster Recovery

- Restoration of Data and Programs
 - Restoration from backup tapes: Need backup tapes at the remote recovery site
 - Real-time journaling (copying each transaction in real time)
 - Database replication

Disaster Recovery

- Testing the Disaster Recovery Plan
 - The importance of testing: Find problems, work faster
 - Walkthroughs
 - Go through steps in real time as group but do not take technical actions
 - Fairly realistic
 - Unable to catch subtle problems

Disaster Recovery

- Testing the Disaster Recovery Plan
 - Live testing
 - Full process is followed, including technical steps (data restoration, etc.)
 - High cost
 - Realistic and can catch subtle errors

Etik

- Systemadministration er et betroet job
- www.sage.org
 - Code of Ethics
- "Informed consent"
 - brugerne skal kende vilkårene
- Vidner hvis det er nødvendigt at bryde privacy