MTAT.08.021
Systems Administration

L10: Remote Support, Risk Management, Disaster Planning

Lecture
2011-04-28
Experience Report Today

• Automatic answering system with Asterisk
• End of lecture (last 15 minutes)
Remote Support

- **vnc**
  - server (x11vnc)
  - client
- **screen**
- **tunneling these**
- **demo**
Risk Management
(Risk Analysis, Risk Assessment)

- Threat
- Incident
- Assets
- Impact
- Vulnerability
- Countermeasures
Risk Management

Asset (vara)

- anything that has a value for the company (or the customer)
- infrastructure, information (data), applications, knowledge, people, capital ...
- material vs. immaterial
- value can/cannot be expressed in monetary units
Risk Management

Threat \((oht)\)
- potential cause of an incident
- unintentional vs. intentional
- passive vs. active

Vulnerability \((nõrkus)\)
- weakness in system that can be exploited by a threat
Risk Management

Countermeasures, Security Measures (*turvameetmed*)

- reduce the risk to an acceptable level
- physical, technological, organizational
- prevent, discover, recover/mitigate
Risk Management

Impact (kahju)
• effect of incidents on assets
• sometimes expressed as a drop in the asset's value
Risk Management

\[ \text{risk} = p(\text{incident}) \times \text{impact} \]
Risk Management

• standards:
  - ISO/IEC 13335, ISO/IEC 27001, 27002 (17799), ISO 31000

• frameworks (+software)
  - Estonia: ISKE
  - Germany: IT-Grundschutz
  - CRAMM methodology and toolkit
Risk Analysis

Qualitative Risk Analysis

- enumerates threats, vulnerabilities, assets, countermeasures
- assigns risk levels to vulnerabilities, threats and assets
- countermeasures are recommended based on these levels
Risk Analysis

Quantitative Risk Analysis

- the process is based on concrete values rather than estimates or levels
- needs probabilities of incidents
- calculates loss expectancies
- more labour-intensive than qualitative analysis
- output suitable for management & finances
- problems with unreliable and inaccurate input
Risk Analysis

- hybrid analysis
  - qualitative + quantitative
- baseline risk assessment (*etalonturve*)
  - pre-assessed risks for common objects
  - includes countermeasures to be implemented for different risk levels
  - Estonia has ISKE
Risk Analysis: Results

• overview of...
  – assets, vulnerabilities, threats, countermeasures
• set of countermeasures to be implemented
• input for disaster planning
• input for security budgeting
Risk Management

- Threat
- Incident
- Assets
- Damage/Impact
- Vulnerability
- Countermeasures
Disaster Planning
Disaster Planning

Mounting root from ufs:/dev/ad0s1a
Re-seeding PRNG: kickstart.
Loading configuration files.
Entropy harvesting: interrupts ethernet point_to_point kickstart.
Swapon: adding /dev/ad0s1b as swap device
Starting file system checks:
/dev/ad0s1a: FILE SYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1a: clean, 153660 free (756 frags, 19113 blocks, 0.3% fragmentation)
/dev/ad0s1d: FILE SYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1d: clean, 991643 free (171 frags, 123934 blocks, 0.0% fragmentation)
/dev/ad0s1f: FILE SYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1f: clean, 18870698 free (180810 frags, 2336236 blocks, 0.7% fragmentation)
/dev/ad0s1e: FILE SYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1e: clean, 3935363 free (53235 frags, 485266 blocks, 0.5% fragmentation)
/dev/ad2s1d: PARTIALLY TRUNCATED INODE I=6947947
/dev/ad2s1d: UNEXPECTED SOFT UPDATE INCONSISTENCY; RUN fsck MANUALLY.
The following file system had an unexpected inconsistency:
ufs: /dev/ad2s1d (/mnt/backup)
Automatic file system check failed; help!
Aug 1 15:01:34 init: /bin/sh on /etc/rc terminated abnormally, going to single
user mode
Disaster Planning

Disaster \textit{(katastroof)} in ITIL: Major Incident

incident, resulting in significant disruption to the service provided by the system or halts the system altogether
Disaster Planning

- hardware failures
- software failures
- power failures
- human errors
- physical environment
  - including temperature and humidity
Disaster Planning

Three most critical recovery resources: backup, backup, backup.
Hardware Failures

- diagnosis is the hardest part
- repair == replace the component
  - repair skills can be learned fast
- spare parts, “donor systems”
- maintenance contracts, warranty
- virtualization :)
Software Failures

• more frequent compared to hardware failures
• operating system errors
• application software errors
• configuration-induced errors
• compatibility problems
• → re-configure, update, implement work-around
• → reporting the bugs
Power Failures

different kinds of power outages and failures

- blackout (täielik katkestus)
- surge, spike (ülepinge, piik)
- brownout (pikaajaline pingelangus)
- frequency instability, harmonic distortions
- noise
Power Failures

• for how long periods must the system be protected?
  - momentary failure: Uninterruptible Power Supply (UPS)
  - 10-30 min: UPS (with enough batteries)
  - 1-10h: UPS + power generator
  - few days: UPS + generator (with enough fuel :))
Uninterruptable Power Supply

• Exercise
  - what types are there
  - How do they work
  - Imagine you build your own cloud (with 500 dualcore computers)
    • what would you need?
  - report
  - 10-15 minutes
Uninterruptible Power Supply

- different UPS technologies
  - off-line (standby)
  - line-interactive
  - on-line (double conversion)
- important UPS parameters
  - power rating
  - protection time
  - types of power failures covered
  - management software
Uninterruptible Power Supply

choosing the UPS

• how much power does your equipment use?
  – to calculate or to measure?
• how long must the system be protected?
• what types of failures must be covered
• big “central” UPS or lots of smaller devices?
• will the UPS be connected to some management and monitoring software?
Emergency Power Generator

• uses ordinary engine fuel
• can only be used in combination with an UPS
• output power rating should be a bit higher than UPS's input power rating
• how will you refuel?
• needs to be serviced on a regular basis
Physical Environment

- high dust levels: overheating, failures in moving parts
- little or no security
- sewage, water, heating pipe failures
- fire hazard
Physical Environment

too high/low temperatures
- the room must have some kind of heating
- use climate control devices

too high/low humidity
- humidity levels should be monitored
- air conditioning systems dry the air
- in our climate - usually there is no need for complicated humidity control devices
Air Conditioning & Climate Control

kliimaseadme võimekus

- cooling capacity
- power rating for systems
- power rating for climate control devices
- in our climate: cold-start option for ACC

in case of power failure...

- air conditioners must be powered by UPS/generator!
Human Errors

End Users
Operators
Administrators
Maintenance Technicians
End User Errors

- very frequent, but low impact
- typical errors
  - deleting or overwriting an important file
  - reckless use of hardware

- train and educate
- manage user rights
- backup
Operator Errors

• more rights → larger impact
• often, outdated or incorrect instructions are to blame

• operators must have up-to-date instructions
• use an auditing system
• backup
Administrator Errors

• super-user access + careless behavior results in a disaster
• possible disasters
  – large-scale data loss or exposure
  – fatal resource exhaustion
• have correct procedures and follow them
• audit, where possible
• backup
• team work
Experience Report

- Automatic answering system with Asterisk