

Informatik für Technische Kaufleute

Alessandro Biotti

Leseprobe

Wings Software Developments
Chaltenbodenstrasse 4 b
CH - 8834 Schindellegi

Tel. +41 43 888 21 51
info@wings.ch
www.wings.ch | www.wings.de



Version

2009 A

Autor

Alessandro Biotti

Art. Nr.

10976.10SG

gebunden

10977.10SL

lose, 4-fach gelocht

Copyright © 1994-2010 Wings Software Developments, alle Rechte vorbehalten.

Diese Kursunterlagen sind urheberrechtlich geschützt. Die Vervielfältigung der Texte und Bilder, auch auszugsweise, ist ohne schriftliche Zustimmung von Wings Software Developments urheberrechtswidrig und strafbar.

Auch Übersetzungen, Mikroverfilmung und Verarbeitung mit elektronischen Systemen sind ohne ausdrückliche Zustimmung von Wings Software Developments nicht erlaubt.

Inhaltsverzeichnis

1	Einleitung	1
1.1	Erläuterungen zum Lehrmittel	1
1.2	Was ist Wirtschaftsinformatik?	1
1.3	Repetitionsfragen	2
2	Systemgrundlagen	3
2.1	Aufbau eines IT-Systems	3
2.2	Von-Neumann-Architektur	3
2.3	Der Mikroprozessor	4
2.3.1	Prozessorarchitekturen	4
2.3.2	Der Arbeitsspeicher	6
2.3.3	Der Festwertspeicher	8
2.3.4	Das Bus-System	8
2.3.5	Die Grafikkarte	8
2.3.6	Der Monitor	9
2.3.7	Die Festplatte	9
2.3.8	Optische Speichermedien	12
2.3.9	Flash-Speicher	12
2.3.10	Peripheriegeräte	13
2.4	Das Betriebssystem	14
2.5	Zeichenkodierung	15
2.5.1	ASCII	15
2.5.2	UTF-8	16
2.6	Repetitionsfragen	17
3	Systemarchitektur	19
3.1	Peer-to-Peer-Architektur	19
3.2	Client-, Server-Architektur	19
3.3	Terminalserver	20
3.4	Clustering	20
3.5	Virtualisierung	20
3.6	Repetitionsfragen	21
4	Informationssicherheit	23
4.1	Vertraulichkeit	23
4.2	Verfügbarkeit	24
4.2.1	Backup-Konzepte	25
4.2.2	RAID-Systeme	25
4.2.3	NAS und SAN	26
4.2.4	USV	27
4.3	Integrität	27
4.4	Repetitionsfragen	29
5	Netzwerkgrundlagen	31
5.1	Was ist ein Netzwerk?	31
5.2	Grösse von Netzwerken	31
5.3	Netzwerktopologien	32
5.4	Kommunikationsarten	34

5.5	Übertragungsmedien	35
5.6	Netzwerkgeräte	36
5.7	Repetitionsfragen	38
6	Netzwerkdienste und Kommunikationsprotokolle	39
6.1	OSI-Modell	39
6.2	Protokolle	40
6.3	Netzwerkdienste	41
6.4	Remote Access Service (RAS)	43
6.5	Repetitionsfragen	44
7	Software	45
7.1	Softwarearten	45
7.1.1	Schichten-Architektur	46
7.2	Funktionsweise einer Software	46
7.2.1	Task und Thread	47
7.2.2	Multitasking	47
7.3	Datenkompression	48
7.4	Wissensmanagement	48
7.5	Programmierung	50
7.5.1	Algorithmus	50
7.5.2	Arten von Programmiersprachen	51
7.6	Datenbanken	52
7.6.1	Relationale Datenbanken	53
7.6.2	Datenbankbegriffe	54
7.6.3	Entity Relation Model (ERM)	55
7.6.4	Transaktionen und Rollbacks	56
7.6.5	Referentielle Integrität	57
7.6.6	Trigger	57
7.6.7	Datenbankabfragesprache SQL	57
7.6.8	Kommerzielle Datenbanksysteme	58
7.7	Lizenzierung	58
7.8	Opensource	59
7.8.1	Definition der Open Source Initiative	60
7.8.2	Wirtschaftliche Bedeutung	60
7.9	Repetitionsfragen	61
8	Projektmanagement	63
8.1	Häufig eingesetzte Projektmanagement-Modelle	63
8.1.1	Wasserfallmodell	63
8.1.2	Spiralmodell (Inkrementelles Vorgehen)	63
8.2	Die grundsätzlichen Phasen von IT-Projekten	64
8.3	Use Case	66
8.4	Eigenheiten von IT-Projekten	67
8.4.1	IT als Disziplin	68
8.4.2	IT als Strategie	68
	Anhang A: vermischte Aufgaben	69
	Anhang B: Kurztest	77
	Anhang C: Lösungen	79
	Index	

4.2.1 Backup-Konzepte

Unter einem Backup versteht man das Sichern von Daten auf ein anders Speichermedium, um im Falle eines Datenverlustes die Daten wiederherzustellen. Die Wiederherstellung von Daten mit Hilfe der Sicherungskopie wird im Allgemeinen als «Restore» bezeichnet.



Die Datensicherung dient dem Schutz vor Datenverlust durch:

- > Hardwareschäden, wie ein Festplattendefekt durch Verschleiss oder externe Einflüsse wie Wasserschäden oder Feuer.
- > Diebstahl oder absichtliche Manipulation der Daten.
- > Computerviren und andere Hacker-Angriffe.
- > Versehentliches Überschreiben oder Löschen von Daten.



Die Daten sollten dabei mindestens einmal pro Tag gesichert werden. Folgende Sicherungsmethoden stehen bei den meisten Backup-Lösungen zur Auswahl:

Vollsicherung

Alle Daten werden gesichert.

Differenzielle Sicherung

Bei einer differenziellen Sicherung werden alle Änderungen seit der letzten Vollsicherung übertragen.

Inkrementelle Sicherung

Hier werden nur diejenigen Daten gesichert, welche sich seit der letzten inkrementellen Sicherung verändert haben.

Eingesetzte Speichermedien sind Bänder und Festplatten.

4.2.2 RAID-Systeme



RAID (**Redundant Array of Independent Disks**) ist ein Organisationssystem von mehreren physikalischen Festplatten eines Computers. Dabei werden mehrere physikalische Festplatten als eine logische Einheit zusammengefasst. Das Ziel von RAID-Systemen ist einerseits die Verfügbarkeit der Daten zu erhöhen und andererseits die Zugriffszeiten auf die Festplatten zu reduzieren.

RAID 0

RAID 0 benötigt mindestens zwei Festplatten. Eine Datei wird in mehrere Teile aufgeteilt und verteilt auf alle Festplatten gespeichert und bei Bedarf wieder von allen Festplatten gelesen. Dadurch werden die Zugriffszeiten stark reduziert. Beispielsweise ist das Lesen und Schreiben auf einer RAID 0 Partition mit drei Festplatten etwa drei Mal so schnell als wenn nur eine Festplatte eingesetzt würde. RAID 0 bietet aber keinen spezifischen Schutz betreffend der Datenverfügbarkeit: Fällt eine physikalische Festplatte aus, sind alle Daten auf allen Festplatten nicht rekonstruierbar.

RAID 1

RAID 1 benötigt genau zwei Festplatten. Eine Datei wird immer parallel auf beide Festplatten geschrieben. Beide Festplatten speichern somit immer dieselben Daten. RAID 1 wird daher auch als **Spiegelung (Mirroring)** bezeichnet. Fällt eine Festplatte aus, so kann das System ohne Unterbruch mit der intakten physikalischen Festplatte weiterarbeiten. Die Zugriffszeiten sind beim Schreiben gleich wie bei einer einzelnen Festplatte, der Lesezugriff ist aber etwas schneller, da parallel von beiden Festplatten gelesen werden kann.

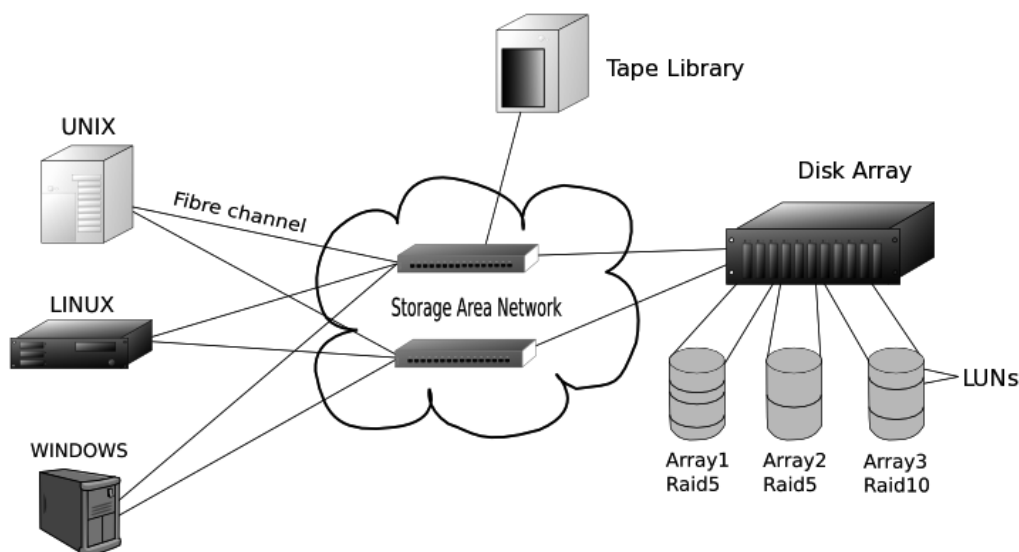
RAID 5

RAID 5 benötigt mindestens drei Festplatten. Eine Datei wird wie bei RAID 0 in mehrere Teile zerlegt und auf alle Festplatten verteilt gespeichert. Eine Festplatte wird hier immer zur Wiederherstellung eingesetzt, so dass beim Ausfall einer Festplatte weitergearbeitet werden kann. Eine defekte Festplatte sollte möglichst schnell ersetzt werden, da bei zwei defekten Festplatten die Daten nicht rekonstruiert werden können. Bei RAID 5 verbessern sich die Zugriffszeiten mit jeder zusätzlichen Festplatte.

4.2.3 NAS und SAN



Ein **Storage Area Network (SAN)** ist ein Netzwerk, über welches Daten zwischen Servern und physikalischen Speicherressourcen transportiert werden. Die grundsätzliche Idee bei SANs ist die Trennung zwischen den verarbeitenden Servern und den eigentlichen Daten. Daten sind bei SANs nicht auf den Servern gespeichert sondern in isolierten Netzwerken (SANs), auf die ein Server zugreifen kann. Ein SAN kann mehrere hundert oder tausend Festplatten verwalten, so dass Daten zentral an einem Punkt gespeichert und gesichert werden können.



Ein **Network Attached Storage (NAS)** ist quasi ein Mini-SAN. Es besteht aus einer oder wenigen Festplatten, die direkt über das Netzwerk angesprochen werden können. Vereinfacht ausgedrückt ist ein NAS eine Festplatte mit Netzwerkanschluss.

4.2.4 USV

Eine **unterbrechungsfreie Spannungsversorgung (USV)**, englisch **Uninterruptible Power Supply (UPS)**, wird eingesetzt, um bei Störungen im Stromnetz die Versorgung kritischer elektrischer Lasten sicherzustellen. Sie besteht aus einer leistungsfähigen Batterie, die in der Lage ist, die zentralen Systeme während einer Übergangsdauer mit Strom zu versorgen. Da eine USV nicht unbeschränkt lange die Systeme mit Strom versorgen kann, schaltet die USV die einzelnen Systeme gemäss einer definierten Prozedur ab, um mögliche Datenverluste und Systemdefekte zu vermeiden.

4.3 Integrität



Integrität besagt, dass Daten über einen bestimmten Zeitraum vollständig und unverändert sein sollen. Eine Veränderung könnte absichtlich, unabsichtlich oder durch einen technischen Fehler auftreten. Integrität umfasst also Datensicherheit (Schutz vor Verlust) und Fälschungssicherheit (Schutz vor vorsätzlicher Veränderung).

Massnahmen zur Sicherung der Integrität

Virenschanner

Ein Antivirenprogramm (auch Virenschanner oder Virenschutz) ist eine Software, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Um Viren aufzuspüren arbeiten Virenschanner mit Signaturen. Jeder Virus besitzt eine eindeutige Signatur (Fingerabdruck) und über diese können Viren schnell identifiziert und beseitigt werden. Daher sollten die Signaturlisten täglich aktualisiert werden, um das System vor neuen Viren zu schützen.

Firewall

Eine Firewall schützt ein privates Netzwerk (LAN) vor einem anderen Netzwerk wie z. B. dem Internet (WAN). Die Firewall überwacht den hindurch laufenden Datenverkehr und entscheidet anhand von Regeln, welche Pakete weitergeleitet werden.

Beispielsweise können Pakete anhand von Softwareports gefiltert werden. Möchte man beispielsweise verhindern, dass Mitarbeiter ausgehende E-Mails mittels SMTP versenden können, so muss man auf der Firewall die Weiterleitung des Ports¹² 25 unterbinden. Folgende Ports werden häufig auf einer Firewall konfiguriert:

¹² Ein Port ist ein logischer Anschluss eines Computers. Jeder Port besitzt eine eindeutige Nummer zwischen 1 und 65535. Häufig wird einem Port ein Protokoll zugeordnet - beim Port 25 ist dies das SMTP (Simple Mail Transport Protocol). Wenn ein Paket bspw. an den Port 25 eines bestimmten Mail-Servers übermittelt wird, dann geht der Server davon aus, dass es sich um eine E-Mail handelt.

4.4 Repetitionsfragen



1. Welche der folgenden Aussagen betreffend Datensicherheit trifft zu?
 - In korrekt installierten Systemen ist ein Systemabsturz unwahrscheinlich, so dass keine besonderen Massnahmen gegen Datenverlust erforderlich sind.
 - Das regelmässige Erstellen von Backups ist eine gute Möglichkeit zur Erhöhung der Datensicherheit.
 - Moderne Betriebssysteme stellen mit der Autorecovery-Funktion in jedem Fall sicher, dass bei einem Systemabsturz keine Daten verloren gehen.
 - Um den Datenverlust bei einem Systemabsturz gering zu halten, ist es sinnvoll, alle Daten vor der Weiterverarbeitung manuell doppelt zu erfassen.

2. Wie viel Prozent der Festplattenkapazität wird bei RAID 1 für die Redundanz der Daten (für die Wiederherstellung im Falle eines Festplattendefektes) verwendet?
 - 0 %
 - 33.3 %
 - 50 %
 - 66.6 %

3. Wie wird das Fachgebiet bzw. die Technologie der Datenverschlüsselung genannt?
 - Hedonismus
 - Einbetten
 - Security
 - Kompression
 - Kryptografie

4. Beim Lesen von Artikeln über das Internet stossen Sie mehrmals auf den Ausdruck «Firewall». Ein derartiges System...
 - ... glättet Netzüberlastungsspitzen.
 - ... steuert die Weiterleitung (Wegwahl) von Datenpaketen auf dem Netz.
 - ... stellt Informationen und Programme für Benutzer eilig bereit.
 - ... übernimmt Aufgaben in der Kommunikation, die vorwiegend mit der Sicherheit verbunden sind.
 - ... dient ausschliesslich der Zwischenspeicherung von favorisierten Adressen.

5. Mit welchen Mitteln oder Software-Lösungen können Sie die Integrität und Verfügbarkeit eines IT-Systems verbessern? Nennen Sie jeweils ein konkretes Beispiel.

6. Am Wochenende erstellen Sie jeweils eine Vollsicherung der Daten, an den Wochentagen (Mo-Fr) führen Sie eine inkrementelle Sicherung mittels Band durch. Wenn am Mittwoch die Daten auf dem Server verloren gehen, welche Bänder benötigen Sie, um die Daten wiederherzustellen?

7. Es gibt diverse Sicherheitsrisiken, vor denen man IT-Systeme schützen sollte. Bekannte Sicherheitsrisiken sind: Computerviren, Trojaner, Würmer, Spoofing, Phishing, Pharming oder Social-Hacking. Wählen Sie drei der aufgeführten Sicherheitsrisiken aus und erläutern Sie jeweils das Sicherheitsrisiko anhand eines Beispiels.