Richtig vernetzt – technische Infrastruktur eines Planungsbüros

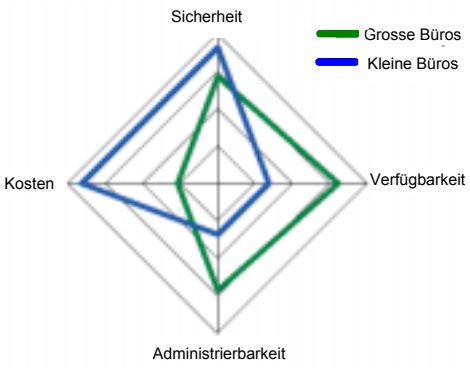
Schnell sind ein paar Rechner aufgestellt, Programme installiert und das Ganze zu einem »peer to peer«[1]-Netzwerk zusammengeschaltet. Doch wenn das Büro wächst, tauchen oft Probleme und Fragen auf: Wie werden unsere Daten gesichert? Ist unser Internetzugang auch sicher? Sind wir vor Viren und Würmern geschützt? Was tun wir bei einem Systemausfall? Spätestens jetzt sollte man sich zum Thema back-office, also zu Server, Gateway, Firewall, Verkabelung, Druckeranbindung, Datensicherung und zentrale Software für Virenschutz, Gedanken machen.
Dieser Artikel soll helfen, diese Komponenten zu verstehen, um derzeitige Konfiguration auf Lücken und Schwächen zu überprüfen oder zumindest mit dem Administrator fundiert diskutieren zu können. Jede einzelne Komponente oder Maßnahme im Netzwerk muss unter den Gesichtspunkten Sicherheit, Verfügbarkeit, Administrierbarkeit und Kosten bewertet werden, die je nach Größe des Büros unterschiedlich gewichtet sind.

Der Server

In einem kleinen Netzwerk genügt in der Regel ein Server. Dieser übernimmt verschiedene Aufgaben:
- Bereitstellung von Dateien (Fileserver)
- Bereitstellung von Druckdiensten (Printserver)
- Autorisierungs- und Rechteserver (Loginserver oder Domain Controller)
- Datensicherung (Backupserver) zentraler Virenschutz

Dazu kommen oft auch folgende Dienste:
- Datenbankdienst (SQL-Server)
- Intranet-Server (Webserver)
- E-Mail-Server

In einem größeren Netzwerk lassen sich die einzelnen Aufgaben einfach auf mehrere Server verteilen. Dadurch steigt die Geschwindigkeit (Performance) und die Verfügbarkeit. Weil ohne Server im Netzwerk nichts mehr läuft, ist besonders auf die Ausfallsicherheit zu achten. Deshalb sollten keine Rechner aus dem Supermarkt verwendet werden, sondern nur speziell als Server ausgewiesene Markengeräte. Diese zeichnen sich durch diverse Merkmale aus:
- Wartungsfreundlicher Gehäuseaufbau mit guter Belüftung (deshalb leider auch laut)
- Starke Netzteile, nach Möglichkeit redundant (zwei unabhängige Netzteile)



Gewichtung der Bewertungskriterien für große und kleine Netzwerke

- spezieller Arbeitsspeicher mit Fehlererkennung (ECC-RAM)
- Motherboard mit eingebauten Diagnose- bzw. monitoring-Möglichkeiten zur rechtzeitigen Erkennung von Hardware-Problemen. Dazu gehören Temperatur, Lüfterdrehzahlen und Spannungen.
- schnelle Netzwerkkarte (Gigalink)
- verlängerte Garantie auf drei Jahre mit zugesicherter Serviceleistung (service level agreement)
- ausfallsicheres Plattensubsystem (RAID)

Besonders dieser Punkt bedarf weiterer Erläuterungen: Da Festplatten elektromechanische Komponenten darstellen, ist die Wahrscheinlichkeit eines Ausfalls höher als bei rein elektronischen Komponenten. RAID-Systeme (Redundant Array of Inexpensive Disks) schaffen hier Abhilfe: Sie verteilen die Daten so auf mehrere Festplatten, dass das System bei Ausfall einer Platte weiter läuft. Daten gehen nicht verloren. Ein RAID-System besteht aus einem Controller (Steckkarte oder Onboard) und mindestens zwei Festplatten.
Die wichtigsten RAID-Level sind:
- RAID 1 (Spiegelung) Hierzu sind zwei identische Platten nötig. Dieses System ist für kleine Server empfehlenswert.
- RAID 5 (Verteilung mit Parität) Hierzu sind mindestens drei Platten nötig. Diese Systeme eignen sich für größere Datei-Server.
- RAID-Systeme lassen sich mit IDE-Platten[2] kostengünstig aufbauen. Wird auf höchste Performance und Sicherheit gesetzt, kommen jedoch vorwiegend die teueren SCSI-Systeme[3] zum Einsatz.

Das Internet-Gateway

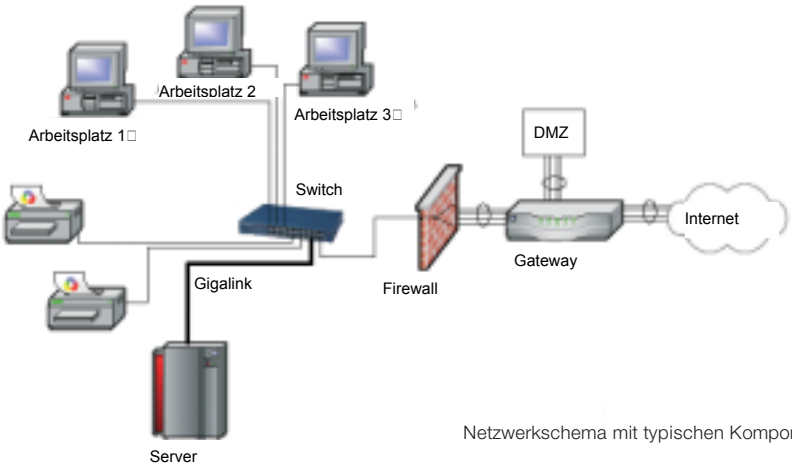
Jedes Büro braucht einen Internetzugang. E-Mail, Datenaustausch, Informationen aus dem Internet und Fernzugänge (Home-Arbeitsplätze) werden damit möglich. Ein kleines Büro ist mit ADSL und einem preiswerten 5 GB Volumentarif gut angebunden und »always on«.
Den Nachteil der nicht statischen IP-Adresse[4] kann man durch Registrierung bei einem dynamischen DNS-Dienst[5] z.B www.DynDNS.org ausgleichen. So ist das Büronetzwerk auch von außen erreichbar für Fernwartung oder FTP-Server[6]. Die Ankopplung des Büro-Netzwerks an das öffentliche Netz sollte durch einen externen Router mit integrierter Firewall erfolgen. Ist der Router richtig konfiguriert, können viele Schädlinge erst gar nicht in das Büronetzwerk eindringen. Diese eingebauten Firewalls arbeiten als Port-Filter und leiten nur explizit freigegebene Ports (Anschlüsse) an Rechner im Netzwerk weiter. In der Firewall sollten die Ports 135 bis 139 sowohl eingehend wie ausgehend blockiert werden. Diese Ports sind für die Veröffentlichung der freigegebenen Ressourcen in Microsoft-Netzwerken zuständig. Auch das DMZ-Feature (Demilitarized Zone) des Routers sollte nicht verwendet werden. Denn ein Rechner, der in der DMZ steht, bekommt alle Internetpakete ungefiltert durchgereicht. Damit alle Rechner im Netzwerk das Gateway auch verwenden können, sollte seine IP-Adresse als Standardgateway auf den Arbeitsstationen eingetragen sein. Solche Standardeinstellungen lassen sich aber auch als Bereichsoptionen über einen DHCP-Server[7] im Netzwerk verteilen.

Die Verkabelung

Eine strukturierte CAT5[8] Verkabelung ist heute Standard. Alte BNC-Netze[9] sollten ausgetauscht werden, da die Geschwindigkeit zu niedrig und die Störanfälligkeit zu hoch ist. Außerdem unterstützen moderne Netzwerkkarten diesen Leitungstyp nicht mehr. Beim Neuaufbau einer Verkabelung differieren die Preise stark zwischen einer einfachen und einer Toplösung:
Lösung 1: Fliegende Patchkabel vom zentralen Switch (Verteiler) zu den Arbeitsstationen. Patchkabel gibt es bis zu 60 Metern Länge vorkonfektioniert. Diese Verkabelung kann aber nur für Büros mit wenigen Arbeitsplätzen empfohlen werden. Die Übersichtlichkeit geht schnell verloren, für jeden neuen Arbeitsplatz muss ein neues Kabel gelegt werden. Die Kosten pro Port inklusive Switch belaufen sich auf nur ca. 40 Euro.
Lösung 2: Fest installierte Kabel vom zentralen Patchpanel (Anschlussfeld) zu den einzelnen Arbeitsgruppen, dort Unterverteilung mit preiswerte SoHo-Switches[10]. Nachteile: eine Arbeitsgruppe teilt sich die Bandbreite zum Server, das Netz kann nicht für Telefonie verwendet werden. Kosten pro Port: ca. 100 Euro.
Lösung 3: Fest installiertes Doppelkabel vom Patchpanel zu jedem Arbeitsplatz. Vorteile: Übersichtlichkeit, nicht störungsanfällig, hohe Geschwindigkeit, Telefonie über dasselbe Netz, höchste Flexibilität. Kosten pro Arbeitsplatz: ca. 400 Euro.
Trotz der hohen Kosten ist bei einer kompletten Neuinstallation Lösung 3 empfehlenswert. Fest installierte Kabel sollten zukunftssicher ausgelegt sein, d.h. auch kommende Datenraten unterstützen. Gut eignen sich S/STP-Kabel bis 600 MHz. Gigabitkomponenten sind mittlerweile erschwinglich, deshalb sollten zumindest die Server über Gigalinks mit dem zentralen Switch verbunden sein. Für Arbeitsstationen ist nur bei Bildverarbeitungsrechnern aufgrund der großen Datenmengen ein Gigalink sinnvoll. Drahtlose Netze (WLAN) sind kein Ersatz für kabelgebundene Netze. Die Geschwindigkeit wird auch in Zukunft um Faktor 10 niedriger sein als bei drahtgebundenen Netzen, die angegebene Reichweite wird in modernen (Beton-) Bauten oft nicht erreicht. Im Besprechungsraum kann ein WLAN jedoch sinnvoll sein, um auch Besuchern den Zugang zum LAN[11] zu ermöglichen.

Druckeranbindung

Drucker, die allgemein verfügbar sein sollen, werden am besten direkt (per TCP-IP) ans Netz gekoppelt. Alle für Arbeitsgruppen ausgelegte Drucker verfügen über diese Option. Dadurch werden sie räumlich vom Server unabhängig. Der Server verwaltet die Warteschlange der Druckaufträge und verteilt bei Bedarf den Treiber im Netzwerk. So muss der Druckertreiber



Netzwerkschema mit typischen Komponenten

nur an einer Stelle gepflegt werden. Drucker ohne Netzwerkoption eignen sich nur als reine Arbeitsplatzdrucker. Diese sollten im Netzwerk nicht freigegeben werden, da weder Mechanik noch Treiber der höheren Belastung im Netzwerkbetrieb gerecht werden.

Virenschutz

Auf dem Server sollten nur speziell für Server entwickelte Virenscanner installiert werden, die jede abgelegte Datei in Echtzeit scannen. Die Virensignaturdatei wird jede Nacht über ein automatisches Update auf den neuesten Stand gebracht. Spezielle Beachtung muss man Notebooks schenken, die auch außerhalb des Büros betrieben werden. Auf diesen Geräten wird zusätzlich ein lokaler Virenscanner eingerichtet, um das Einschleppen von Viren zu verhindern. Häufige Infektionsquelle sind E-Mails. Hier ist vor allem die Aufklärung der Mitarbeiter wichtig: keine Post von unbekannter oder zweifelhafter Herkunft öffnen, keine Anhänge mit den Endungen .exe, .com, .bat, .cmd, .vbs, .js, .pif akzeptieren. Viele Provider bieten virengescannte Postfächer an. Betreibt man ein eigenes Mail-Gateway sollte es mit einem Virenscanner Plugin ausgestattet sein. Vor bekannten Viren ist das Netz damit weitestgehend sicher. Doch wie kann man es vor neuen, unbekannten Viren schützen? Viele Programmhersteller bieten einen Newsletterdienst an, der über neue Viren informiert. Die hier vorgeschlagenen Maßnahmen, z.B. Einspielen von Sicherheits-Updates oder Sperren von Ports in der Firewall, sollten zeitnah umgesetzt werden.

Datensicherung

Trotz aller Vorkehrungen, um ein System vor Ausfällen zu schützen, ist eine regelmäßige Datensicherung unerlässlich. Diese sollte möglichst automatisch ablaufen und die Bänder an einem sicheren Ort aufbewahrt werden. Am häufigsten ist die Wiederherstellung von einzelnen, versehentlich gelöschten Dateien notwendig. Eine komplette Bandsicherung schützt aber auch vor Vandalismus, Diebstahl, Feuer oder schwerwiegendem menschlichem und technischem Versagen. In solchen Fällen führt eine fehlende Bandsicherung schnell in den Konkurs. Als Sicherungsmedium kommen vor allem zwei Bandtypen in Frage: DDS-Tapes bis 20 GB unkomprimierter Kapazität. (Die Laufwerke verwenden ein Schrägspuraufzeichnungsverfahren mit rotierendem Kopf. Deshalb ist der Verschleiss am Gerät relativ hoch.) DLT-Tapes von 40 GB bis 160 GB unkomprimierter Kapazität. (Die Laufwerke verwenden ein Parallelspuraufzeichnungsverfahren. Sowohl Bänder als auch Gerät sind dadurch robuster.) Als bewährtes Sicherungsschema gilt: Freitag nacht Komplettsicherung, Montag bis Donnerstag differenzielle Sicherung, d.h. jede Tagessicherung beinhaltet alle Änderungen bis zur letzten Vollsicherung. Für die Komplettsicherung kommen mindestens drei Wochenbänder und 12 Monatsbänder rotierend zum Einsatz. Auf diese Weise lassen sich Dateien über einen Zeitraum von einem Jahr zurückverfolgen. Neben dieser Bandsicherung, die vor allem dem »Disaster recovery« dient, leistet auch eine zusätzliche, differenzielle Kopie aller Nutzdaten auf eine zweite Maschine im Netzwerk gute Dienste. Diese Kopie kann entweder durch eine XCOPY-Script[12] oder durch ein Synchronisationstool wie z.B. »robocopy« erfolgen. Da auf diese Sicherung einfach über den Explorer zugegriffen werden kann, sind versehentlich gelöschte oder überschriebene Dateien schnell wieder hergestellt. Zwei einfach anpassbare Sicherungsscripte finden Sie auf unten genannter Homepage zum Download.

Armin Winter

[1] peer to peer: Netzwerk ohne dedizierten Server
[2] IDE (integrated drive electronics): Anschlussart bei preiswerten Festplatten
[3] SCSI (small computer system interface): Bussystem der mittleren Datentechnik
[4] IP-Adresse (Internet protocol address): Nummernsystem zur eindeutigen Kennzeichnung von Rechnern im Netzwerk
[5] DNS-Dienst (domain name service): Auflösung von Namen in IP-Adressen
[6] FTP-Server (file transfer protocol): einfacher Dateiaustauschdienst
[7] DHCP-Server (dynamic host configuration protocol): Dienst zur automatischen Vergabe von IP-Adressen im Netzwerk
[8] CAT5: Norm für Netzwerkkabel
[9] BNC (bayonet navy connectory): koachsialer Kabeltyp
[10] SoHo (small office home office): Komponenten für kleine Büros oder Heimarbeitsplätze
[11] LAN (local area network): lokales Netzwerk
[12] XCOPY: leistungsfähiger Kopierbefehl

Der Autor ist seit 1986 als herstellerunabhängiger Systemberater und -betreuer für Architektur- und Planungsbüros in München tätig. Seit 2001 betreibt er zudem eine Plattform für internetbasiertes Projektmanagement im Bauwesen unter: www.flumen.de