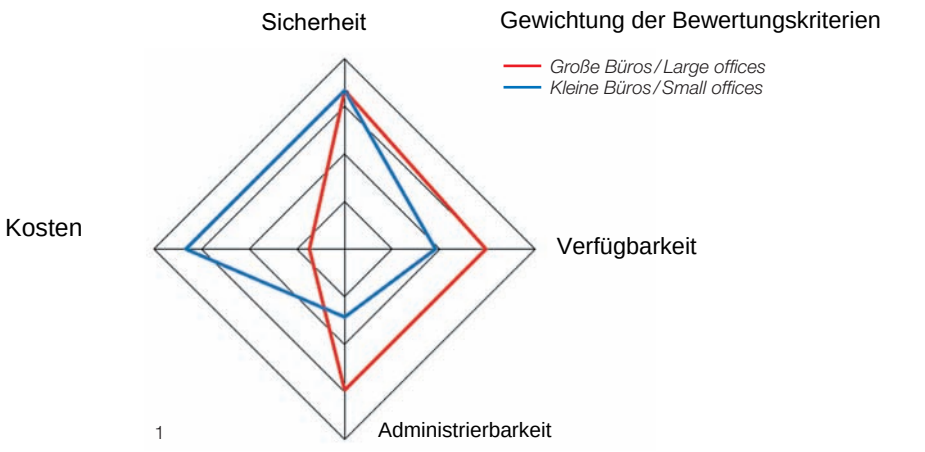
**Richtig vernetzt –
IT-Strukturen für Planungsbüros**

**Properly Networked –
IT Structures for Planning Offices**

Armin Winter



1

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« Gedanken machen, also zu Server, Gateway, Firewall, Verkabelung, Druckeranbindung, Datensicherung und zentraler Software für Viren- und Spamschutz.
Der vorliegende Artikel soll dazu beitragen, diese Komponenten zu verstehen, existierende Konfigurationen auf Lücken und Schwächen zu überprüfen oder zumindest mit dem Administrator fundiert diskutieren zu können. Jede einzelne Komponente oder Maßnahme im Netzwerk muss dabei unter den Gesichtspunkten Sicherheit, Verfügbarkeit, Administrierbarkeit und Kosten bewertet werden. Diese sind je nach Größe des Büros unterschiedlich gewichtet.

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 / Domain Controller)
- Datensicherung (Backupserver)
- zentraler Virenschutz

Hinzu 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 steigen Geschwindigkeit (Performance) und 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)
- 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)
- Möglichkeit der Fernwartung über speziellen Remote Controller
- ausfallsicheres Plattensubsystem (RAID)

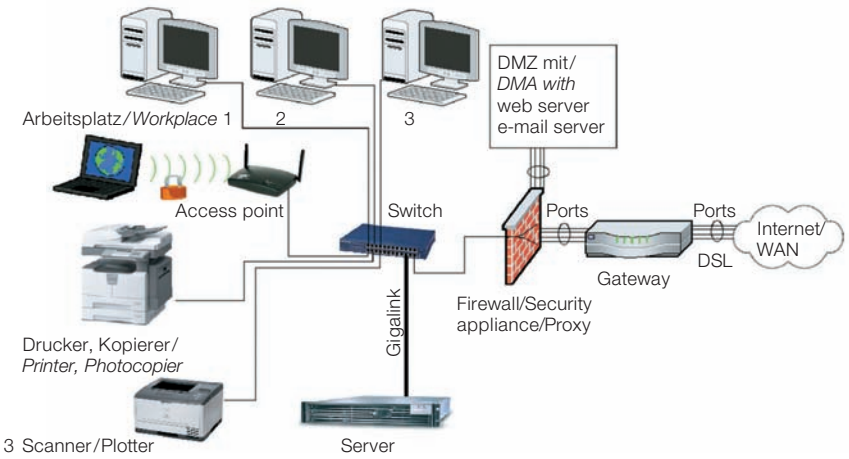

2

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 weiterläuft. 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) mit zwei identischen Platten. Dieses System ist für kleine Server empfehlenswert. RAID 5 (Verteilung mit Parität) eignet sich für größere Systeme und beansprucht mindestens drei Platten.
RAID-Systeme lassen sich mit SATA-Platten[2] kostengünstig aufbauen. Wird auf höchste Performance und Sicherheit gesetzt, kommen jedoch vorwiegend die teueren SCSI-Systeme[3] zum Einsatz.

Das Internet-Gateway
Für E-Mail, Datenaustausch, Informationen aus dem Internet und Fernzugänge (Home-Arbeitsplätze) benötigt jedes Büro einen Internetanschluss. Kleine Büros sind mit einer asymmetrischen DSL (ADSL) mit mindestens 1 MBit Upstream und 6 MBit Downstream und einem flat-Tarif 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) teilweise ausgleichen, der einfache Serverdienste wie FTP[6] oder Fernwartung ermöglicht.
Größere Büros, die erweiterte Serverdienste wie z.B Groupware-Lösungen, eigenen E-Mail Server oder LAN-LAN-Kopplung per VPN[7] betreiben wollen, sollten eine symmetrische DSL (SDSL) mit mindestens 2 MBit Up/Downstream wählen. Hier ist dann auch ein festes IP-Subnetz enthalten, sodass wichtige Server und Dienste direkt aus dem Internet erreichbar gemacht werden können. Vor allem E-Mail-Server sollten mit einer öffentlichen, nicht dynamischen IP-Adresse konfiguriert werden. Viele E-Mail-Server ak-zeptieren nämlich Post von Servern mit dynamischer IP-Adresse aus Gründen des Spamschutzes nicht mehr.

Die Ankopplung des Büro-Netzwerks an das öffentliche Netz erfolgt im einfachsten Fall, also dem ADSL, durch einen Router mit integrierter Firewall und NAT (Network address translation). Ist der Router richtig konfiguriert, können viele Schädlinge erst gar nicht in das Büronetzwerk eindringen. Diese ein-

DETAILtopics: weiterer Artikel »Software für Planungsbüros«: www.detail.de/0011



1 Gewichtung der Bewertungskriterien für große und kleine Netzwerke
2 Höchstleistungsrechner Leibniz-Rechenzentrum Garching
3 Netzwerkschema mit typischen Komponenten
4 Server Leibniz-Rechenzentrum Garching

1 Evaluation of criteria for large and small networks
2 Top-speed computer at Leibniz Computer Centre, Garching
3 Network diagram showing typical components
4 Server in Leibniz Computer Centre, Garching

fachen Firewalls arbeiten als Port-Filter und leiten nur explizit freigegebene Ports (Anschlüsse) aus dem Internet = WAN (wide area network) an Rechner im lokalen Netzwerk (LAN = local area network) weiter. In der Firewall sollten zumindest die Ports 135 bis 139 sowohl eingehend wie ausgehend blockiert werden. Diese Ports sind für die Veröffentlichung der freigegebenen Ressourcen in Microsoft-Netzwerken zuständig. Bleiben diese Ports offen, ist möglicherweise der gesamte Datenbestand von Unberechtigten einsehbar.
Auch das DMZ-Feature (Demilitarized Zone) solch einfacher Router sollte höchstens für Testzwecke verwendet werden, da ein Rechner, der in der DMZ steht, alle Internetpakete ungefiltert durchgereicht bekommt und nicht hinreichend vom LAN abgetrennt ist. Solche einfachen Gateways kosten ca. 200 Euro und werden vom Internet Service Provider meist subventioniert angeboten. Beim symmetrischen DSL mit festem Subnetz wird der Router meist vom Provider gestellt und konfiguriert. Diese Router leiten alle ankommenden Pakete unbearbeitet und ohne Filterung oder NAT an die interne Schnittstelle weiter. Somit ist hier eine nachgeschaltete, separate Firewall oder Security Appliance zwingend notwendig. Unter dem Schlagwort Security-Appliance bieten immer mehr Hersteller fertige, oft Linux-basierte Sicherheitslösungen an, die als Black Box das gesamte Sicherheitsmanagment, also Firewall, Virenschutz, Content-Filter sowie Intrusion-Detection übernehmen. Über einen Updateservice bleibt die Box immer auf dem aktuellen Stand.

Die Netz-Infrastruktur
Bei der Planung einer Netzwerk-Verkabelung sollten folgende Aspekte berücksichtigt werden: Server, Switch, Firewall, Router benötigen eine staubfreie Umgebung mit optimalen 20 °C. Ideal ist ein zentral gelegener, abgeschlossener Serverraum mit 19 Zoll-Rack, in dem alle Komponenten übersichtlich angeordnet sind. Ist dies nicht möglich, kann ein geschlossener Serverschrank mit entsprechenden Luftfiltern und Lüftern zum Einsatz kommen. Bereits kleine Installationen erreichen Wärmelasten von 800 Watt, die abtransportiert werden müssen. Das kann entweder durch hohen Luftaustausch (der aber Staub produziert), oder durch ein möglichst eigenständiges oder zumindest separat regelbares Klimagerät erfolgen, das rund um die Uhr betriebsbereit sein muss. Bei niedriger Temperatur und staubfrei laufen Server deutlich länger.
Jeder Arbeitsplatz benötigt zwei Netzwerkanschlüsse für Rechner und Telefon. Neue Komponenten und Kabel sollten Kategorie 6 entsprechen, weil dieser Standard auch für die kommenden 10 Gbit Netzwerke geeignet sein wird. Alle Kabel sollten im Serverraum zusammenlaufen. Reichen die zugelassenen 100 m pro Kabelsegment nicht aus, sind aktive Unterverteilungen nötig. Pro Arbeitsplatz kostet der Doppelanschluss inklusive Switchport ca. 400 Euro.
Drahtlose Netze (WLAN) sind aufgrund ihrer niedrigeren Geschwindigkeit kein Ersatz für kabelgebundene Netze. Oft entspricht die vom Hersteller angegebene Reichweite (besonders in Betonbauten) nicht der Realität. Ein WLAN kann dennoch eine sinnvolle Ergänzung sein, um z.B. Besuchern im Besprechungsraum einen Netzzugang zu eröffnen oder um Notebooks mobil und ohne Kabel einzubinden.

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, die sie räumlich vom Server unabhängig macht. Der Server verwaltet die Warteschlange der Druckaufträge und verteilt bei Bedarf den Treiber im Netzwerk. So muss der Druckertreiber nur an einer Stelle gepflegt werden. Drucker ohne Netzwerkoption eignen sich nur als reine Arbeitsplatzdrucker. Sie sollten im Netzwerk nicht freigegeben werden, da weder Mechanik noch Treiber der höheren Belastung im Netzwerkbetrieb gerecht werden. Moderne Kopierer lassen sich auch als Drucker und Scanner ins Netzwerk einbinden. Speziell bei Farbkopierern gewinnt man so einen deutlichen Mehrwert.

Telefonie
Telefonanlagen basieren heute noch größtenteils auf ISDN. Doch VOIP (Voice-over-IP) ist inzwischen den Kinderschuhen entwachsen und kann nicht nur durch erhebliche Einsparungen bei den Gebühren punkten. Auch die möglichen funktionalen Leistungsmerkmale, Flexibilität der Konfiguration und Zukunftssicherheit durch offene Standards sprechen für VOIP, beispielsweise die transparente und gebührenfreie Einbindung von Zweigstellen oder Heimarbeitsplätzen an die Telefonanlage. Die Mitarbeiter sind dabei immer unter der gleichen Nebenstelle erreichbar. Leistungsmerkmale wie Warteschlangen, Konferenzschaltung, individuelle Voicemailbox, Parallelklingeln, Wählen per Mausklick (CTI) waren bisher teuren Telefonanlagen vorbehalten.
Folgende Varianten eines Wechsels zu VOIP sind möglich:
- Die bestehende Telefonanlage wird weiterbetrieben und mit einem VOIP-Gateway ergänzt. Dadurch können zumindest die Gesprächsgebühren reduziert werden.
- Die Telefonanlage wird durch eine VOIP-Anlage ersetzt und selbst gemanagt.
- Man verzichtet völlig auf eine eigene Telefonanlage und nutzt die Dienste einer Hosted PBX (Privat Branch Extension = Telefonanlage). Die Variante ist vor allem für kleinere Büros interessant.

Bei allen Vorzügen einer VOIP-Anlage darf man einen Nachteil nicht übersehen: Durch die Zusammenlegung von Daten- und Sprachdiensten auf eine technologische Grundlage sinkt die Diversität. Eine redundante Internetanbindung und entsprechende SLA (Service Level Agreements) können diesen Punkt entschärfen.

Virenschutz
Auf dem Server sollten nur speziell für Server entwickelte Virenscanner installiert werden, die jede abgelegte Datei in Echtzeit scannen. Die Virensignaturdatei wird jede

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. www.flumen.de

Since 1986, the author has worked independently of manufacturing companies as a system consultant and supervisor to architectural and planning offices in Munich. Since 2001, he has also provided a platform for internet-based project management in building www.flumen.de

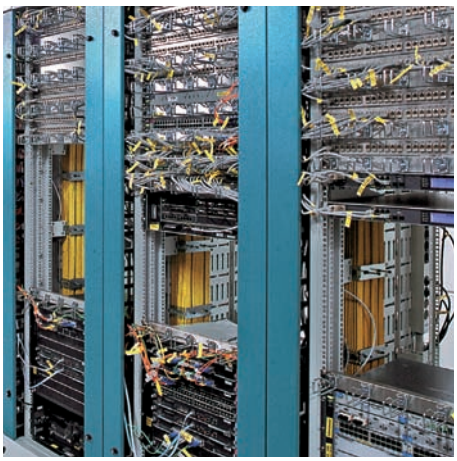
Anmerkungen
[1] peer to peer: Netzwerk ohne dezidierten Server
[2] SATA (Serial Advanced Technology Attachment): Anschlussart bei preiswerten Festplatten
[3] SCSI (Small Computer System Interface): Bussystem
[4] IP-Adresse (Internet Protocol Address): Nummernsystem zur eindeutigen Kennzeichnung von Rechnern im Netzwerk
[5] DNS-Dienst (Domain Name Service): Auflösung von Namen in IP-Adressen
[6] FTP (File Transfer Protocol): einfacher Dateiaustauschdienst
[7] VPN virtuelles privates Netzwerk: Nutzung des Internets zur getunnelten geschützten Übertragung privater Daten

Notes
[1] Peer-to-peer: network without dedicated server
[2] SATA (serial advanced technology attachment): form of connection with low-cost hard disks
[3] SCSI (small computer system interface): bus system
[4] IP address (internet protocol address); numerical system for individual registration and identification of computers in a network
[5] DNS (domain name service): conversion of names into IP addresses
[6] FTP (file-transfer protocol): simple file-exchange system
[7] VPN (virtual private network): use of internet for tunnelled, protected transmission of private data

Nacht über ein automatisches Update auf den neuesten Stand gebracht. Spezielle Beachtung muss man Notebooks schenken, die auch außerhalb des Büros betrieben werden. Sie benötigen zusätzlich einen lokalen Virenscanner, 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 Plug-in ausgestattet sein. Vor bekannten Viren ist das Netz damit weitestgehend sicher.
Gegen neue, unbekannte Viren bieten viele Programmhersteller einen Newsletterdienst an. Die hier vorgeschlagenen Maßnahmen, z. B. Einspielen von Sicherheits-Updates oder Sperren von Ports in der Firewall, sollten zeitnah umgesetzt werden.
Neu entdeckte Sicherheitslücken werden von professionellen Hackern inzwischen in großem Stil systematisch ausgenutzt. Auf allen Systemen sollten daher zumindest sicherheitskritische Updates automatisch und täglich eingespielt werden. Im (Microsoft-) Netzwerk gibt es dafür den Serverdienst WSUS (Windows Software Update Service), der die zentrale Verwaltung, Freigabe und Verteilung von Softwareupdates ermöglicht.

Spamschutz
Effektiver Schutz vor Spam ist heute ein wichtiges Kriterium. Da die Techniken der Spammer immer raffinierter werden, wächst auch der Aufwand, einen guten Spamfilter zu betreiben. Zunächst einige Tipps, wie Sie Ihre E-Mail-Adresse vor Spammern möglichst »geheim« halten können:
- Legen Sie sich für zweifelhafte Kontakte eine Dummy-Adresse bei einem Freemailer zu. Diese Adresse können Sie dann gelegentlich einfach ändern.
- Verwenden Sie die echte Email-Adresse nur mit seriösen Partnern.
- Veröffentlichen Sie Ihre echte Email-Adresse nie im Klartext im Web, z.B auf Ihrer Homepage oder in Foren jeglicher Art. Roboter scannen das Web systematisch nach E-Mail-Adressen. Verwenden Sie besser ein Bild Ihrer E-Mail-Adresse.

Spamfilterung ist an verschiedenen Stellen möglich:
- Beim ISP, der ihre Mailboxen betreibt
- Auf Ihrem eigenen Mail/Exchange-Server
- Auf einer Ihrem Netzwerk vorgeschalteten Security appliance
- Über spezialisierte Onlinedienste, die als Zwischenstation die Überprüfung der eigenen Mailboxen übernehmen.


4

Datensicherung
Trotz aller Vorkehrungen, ein System vor Ausfällen zu schützen, ist eine regelmäßige, möglichst automatisierte Datensicherung auf externe Medien unerlässlich. Diese sollten an einem sicheren Ort, am besten außerhalb des Büros, aufbewahrt werden. Am häufigsten ist die Wiederherstellung von einzelnen, versehentlich gelöschten Dateien nötig. Eine komplette Datensicherung schützt aber auch vor Vandalismus, Diebstahl, Feuer oder schwerwiegendem menschlichen und technischen Versagen. Ein Desaster Recovery Plan sollte notwendige Handlungsschritte für solche Fälle beinhalten mit dem Ziel, möglichst schnell wieder ein lauffähiges (Not-) System auf die Beine zu stellen.
Als Sicherungsmedium kommen die bislang benutzten Bänder immer mehr aus der Mode. Sie werden durch die vergleichsweise komfortable Sicherungen auf preiswertere, externe Festplatten ersetzt. Ein weiterer Pluspunkt ist die Möglichkeit einer Synchronisation, bei der nur geänderte Daten kopiert werden. Das spart Zeit und schont die Festplatten in den Servern. Bei einer vollständigen Datensicherung auf Band muss dagegen immer der gesamte Datenbestand gelesen und geschrieben werden. Ein Sicherungsprogramm sollte die synchronisierende Datensicherung unterstützen. Aber auch mit ein paar Zeilen VBS-Script lassen sich automatisch ablaufende Sicherungsschemen erstellen.
Als bewährtes Sicherungsschema gilt: Freitagnacht Komplettsicherung, Montag bis Donnerstag differenzielle Sicherung, d.h. jede Tagessicherung beinhaltet alle Änderungen bis zur letzten Vollsicherung. Die Komplettsicherungen sollten mindestens drei Monate zurückreichen.
Zusätzlich zu den externen Sicherungen gibt es bei Windows-basierten Servern ab 2003 die Möglichkeit der »Schattenkopien«, womit sich frühere Versionen von Dateien direkt aus dem Explorer heraus wiederherstellen lassen. Dieser Mechanismus schützt vor allem vor versehentlichem Überschreiben bzw. Löschen von Dateien.
Die allgemeine Sicherung ersetzt natürlich nicht eine projektbezogene Archivierung von wichtigen Planungsständen. Diese kann auf DVD erfolgen und wird direkt im Projektordner abgelegt.

Fazit
Jeder Büroinhaber muss letztendlich selbst entscheiden, welche Anforderungen er an seine IT-Infrastruktur stellt und wieviel er dafür investieren will. Für den Mitarbeiter stellt der Rechner das wichtigste Arbeitsgerät dar. Nur wenn Gerät, Software und die dazugehörigen Dienste im Hintergrund reibungslos zusammenspielen, wird er die bestmögliche Produktivität erzielen.

Setting up a few computers, installing programs and establishing a peer-to-peer[1] network is quickly done; but when an office expands, problems often arise: safeguarding data and internet access, viruses and other matters. This article is meant to help readers understand the various components of such systems, therefore.

Servers have the function of providing access to files and data (file server) and to printing facilities (printing server). They protect data (back-up server) and act as a central control shield against viruses. In addition, servers provide a databank service (SQL server) and afford access to the web and e-mail.

In a larger network, these tasks can be distributed over a number of servers, which helps to improve the performance. Since nothing functions in the network without a server, care must be taken to ensure its operation at all times and to allow a certain fault tolerance. That is one reason for not buying computers from the next best supermarket. Brand goods are distinguished by a number of different features:

- *they are easier to maintain;*
- *ideally they should contain two independent power-supply units;*
- *they should contain a special random access memory with a facility for recognizing errors (ECC-RAM);*
- *they should incorporate a motherboard with the ability to anticipate hardware problems;*
- *they should contain a fast-functioning network circuit (gigalink); and*
- *there should also be a hard-disk subsystem (RAID) (redundant array of inexpensive disks).*

Since hard disks are electro-mechanical components, there is a greater likelihood of failure than with purely electronic elements. RAID systems provide one form of assistance in this respect by distributing data over a number of hard disks, thereby helping to prevent losses. A RAID system consists of a controller and at least two hard disks, and it can be extended economically with SATA- disks[2]. For the best performance and safety, expensive SCSI systems[3] should be chosen.

Every office needs an internet link. Smaller offices will manage very well with an asymmetric DSL (ADSL) with at least 1 MByte upstream and 6 MBytes downstream, and operating on a flat-rate always-on basis. Larger offices that require extended server facilities, with their own e-mail server or LAN-LAN connection per VPN[7], should opt for a symmetric DSL (SDSL) with a minimum of 2 Mbytes upstream/downstream.

Linking the office network with the public network can, in the simplest case (i.e. ADSL), be effected by means of a router with integrated firewall and network address translation (NAT). With a proper configuration of the router, many parasites will have no access to the office network. At least the ports 135–139 in the firewall should be blocked against entry and exit. If these ports remain open, the entire data will possibly be accessible to unauthorized persons.

In the case of symmetric DSL with a fixed subnet, the router is usually supplied and configured by the provider. These routers forward all incoming packages to the internal interface unprocessed and without filtering or NAT. Here, too, a separate downstream firewall or security appliance is essential. More and more companies offer security appliances – often with Linux-based safety systems – in the form of a black box that provides the entire security management (i.e. firewall, virus protection, content filter and intrusion detection). An update service allows the box to keep abreast of developments.

When planning the cable runs for a network, the following aspects should be taken into account: the server switch, firewall and router require a dust-free environment with an optimum temperature of 20 °C. A central, enclosed server room with a 19-inch rack providing easy access to all components is ideal. If this is not possible, a closed server cupboard with the appropriate air filters and ventilation can be installed. Even small-scale installations can cause heat loads of 800 W, which have to be removed.

Every workplace needs two network connections for the computer and telephone. New components and cables should comply with category 6, since this will be the standard for 10-Gbyte networks in the future. A twofold connection, including a switchport, costs roughly €400 per workplace.

In view of their slower speed, wireless networks (WLAN) are no substitute for cable-linked systems. In many cases, their range is less than that stated by the manufacturer, particularly in concrete structures. A WLAN can nevertheless provide a useful complement to other systems.

Printers for general use should ideally be directly linked to the network. All printers installed for working groups have this option, which makes them spatially independent of the server. The server coordinates the queue of printing orders. Printers without a network option are suitable solely for individual workplaces. Modern copying machines can also be integrated in the network and used as printers and scanners. This is particularly useful in the case of colour copying.

Nowadays, most telephone installations are based on ISDN. In the meantime, though, VoIP (voice-over IP, i.e. phoning via the PC and internet) has advanced beyond the teething stage and offers many advantages, including savings in charges, flexibility in the configuration and security for the future. For example, transparent integration of phone extensions and home workplaces with no extra costs for phone installations mean that staff and assistants can always be reached on the same extension. Other features such as waiting loops, conference connections, individual voicemail boxes, dialling per mouseclick (CTI), etc. are feasible today and at much more reasonable rates than in the past. Telephone networks can also be replaced with the services of a hosted private branch extension (PBX), an alternative that is of interest especially to smaller offices. One disasdvantage of VoIP installations, however, is that by basing data and spoken communication services on a single technology, diversity is reduced.

Only virus scanners that have been specially developed for servers and that scan every stored file in real time should be installed in a server. Virus signature files are automatically updated every night. Special attention must be paid to notebooks that are used outside the office. They require an additional local virus scanner. E-mail is a common source of virus infection, and staff should be instructed to this effect. If a firm has its own mail gateway, it should be fitted with a plug-in virus scanner.

Effective protection against spam is an important factor nowadays. Various methods can be used to filter it out. A dummy address can be set up with a freemailer for dubious contacts. The address can be changed from time to time. A genuine e-mail address should be given only to serious partners and should never be freely advertised on one's home page on the web. Spam can be filtered out at a number of points, such as in the ISP that operates the mailboxes, in one's own mail/exchange server, via a security appliance, or by means of specialized online services.

To protect a system against losses, a regular process of data storage on external media is essential. This should function automatically if possible and be housed in a safe place, ideally outside the office. Most commonly, the retrieval of wrongly deleted data is required, but a complete data-security system also protects against vandalism, theft, fire, human error and technical failure. A disaster recovery plan should ensure the necessary steps for the swift instatement of an emergency system.

The practice of employing used tapes is slowly yielding to a comparatively comfortable system of storing data on more economical external hard disks. A further advantage of this is the scope it provides for synchronization, whereby only changed data are copied, thus saving time and also wear on the hard disks. One well-tried security system consists of a complete saving of data on Friday evening, with differential saving from Monday to Thursday. The complete saving should extend back over at least three months. In addition to external storage, Windows-based servers have provided for "shadow copying" since 2003.

Ultimately, all office owners must decide for themselves what demands they make of their IT infrastructure and how much they wish to invest for this purpose. Only when the appliance, software and the related services are coordinated and function smoothly with each other can maximum productivity be achieved.