SECURE WAN COMMUNICATION FOR TELEWORKERS. A CASE STUDY.

Hörmanseder Rudolf, Mühlbacher Jörg R.
FIM - Institute for Information Processing and Microprocessor Technology,
Johannes Kepler University Linz, A-4040 Linz, Austria
syspro@fim.uni-linz.ac.at

Abstract. This paper describes the structure of a typical situation in which tele-workers / freelancers work for several companies from their private home office. Particular emphasis is given to low cost solutions without sacrificing security issues, which are of increasing importance. We describe the initial state and explain the steps of the solution in detail. Issues such as VPNs, firewalls and ISPs are included in order to meet the needs of both tele-workers / freelancers and contracting companies.

Keywords. Telecommunication, Teleworking, Tele-Cooperation, WAN, Wide Area Network, IPSec, VPN, Virtual Private Network, Firewall, IT-Security, Network Security

INTRODUCTION

New forms of labour and more flexible contracts of employment are becoming more frequent. This social change manifests itself in flexible working conditions and working hours, short-time employment for different companies or new forms of self-employment and an increasing dissolution of the boundary between job and private life.

The structure of IT solutions has to reflect these changes. So specific home-offices / tele-offices with IT equipment and connection to the Internet are becoming more and more common. Current telecommunication technology offers low-cost solutions that allow staying online all day. The communication structure resulting from these changes leads to new security requirements for tele-offices, which are similar to companies. Also, companies co-operating with tele-workers and freelancers recognise additional specific security requirements and therefore have to adapt their IT and security policy to these new needs.

In this paper we discuss general requirements for tele-worker, before listing some main steps towards a stable solution. Then a small case study, which is based on well-known standards and knowledge, illustrates a feasible solution. Minimal additional costs while not neglecting fundamental security and availability requirements are the main goals. Reasons for several decisions made in the case study are described. The solution is then compared with general requirements.

GENERAL REQUIREMENTS

General communication needs for tele-workers.
We start with a summary of tele-working features that are relevant to the rest of the paper.

Reuse of resources and scalability. Tele-workers want to use their available (old) equipment in their SOHO (=small office / home office) environment. Because workload and accompanying demands grow gradually, home-offices often start with one computer and are continually expanding towards a local area network with connection to the Internet.

Interleaved work. Tele-workers, in particular self-employed persons and freelancers, often work for more than one company at the same time. So an online connection to every contractor should be available simultaneously or at least interleaved connection must be provided. These online connections shall not (or only as far as absolutely necessary) depend on the IT platforms, which are used in the contracting companies.

Access from company to home-office. Sometimes tele-workers have to work temporarily - "physically" - at a company's premises. In that case, they also need (at least) limited access to their resources at home, e.g. for downloading files they need. Also, trusted access to the tele-worker's office LAN must be provided for the contracting companies (to some extent).

General Internet access. We assume that every tele-worker needs Internet access at least for (a) advertising her-/himself on the net, (b) information search and (c) e-mail.

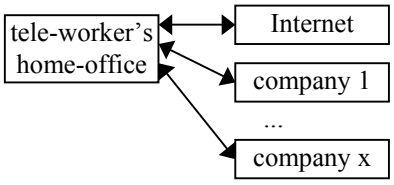

Fig. 1. General communication requirements

Figure 1 summarises the communication requirements of a typical self-employed tele-worker. Employees of a company usually have fewer requirements.

Personal security issues.
As every other company, tele-workers have to secure their local IT-environment too. This fact gets more and more important, as many home-offices are online in the Internet all the day.

Additionally, every tele-worker has to protect her/his intellectual work against espionage. This holds for any contracting company too: it should not have unlimited access to local know-how and knowledge other than what has been specified in the agreement. In particular, for self-employed persons this demand for protection is absolutely vital. Employees of a company are not usually concerned with this, because intellectual rights are typically bound to the employer and knowledge within the company should be shared in the interest of the company and work efficiency.

Employers / Contractors security issues
Generally, these mirror the security issues of tele-workers as described in the previous section. Additionally, employers must tailor and restrict access permissions of tele-workers only to those resources that are necessary. So, tele-workers are often only allowed to use resources within an Extranet or in a DMZ (=demilitarised zone). Even then, because there is a kind of trust between home-offices and the company's network, security officers may fear being hacked indirectly via the tele-worker's home-office (see figure 2). Matters may get even more complex e.g. when tele-workers use wireless LANs (e.g. IEEE 802.11b) in their SOHO environments [1].

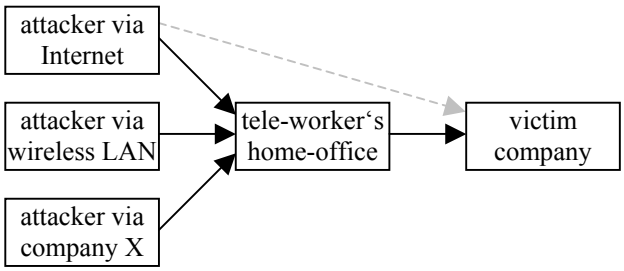

Fig. 2. Possible indirect attacks via contractor to company

To keep security threats of this type as small as possible, the security-officer of a company wants to check all communication between the tele-worker and the Internet and wants to prohibit any communication with other companies (see figure 3 and compare it with figure 1). But an approach such as the one shown in figure 3 would lower the available bandwidth for tele-workers and would provoke additional costs for (two-fold!) data transfer. The imposed limits of this structure are usually too restrictive for self-employed persons, and might be feasible only for internal staff.

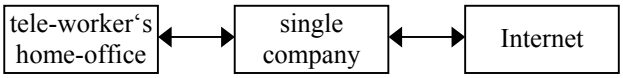

Fig. 3. Restrictive structure (for employees??)

STEPS TOWARDS A STABLE SOLUTION

LAN at the home office
Because the LAN of a SOHO is (by definition) small, there is not too much to say about it. Nevertheless, because the LAN at home often holds/transfers secret business data, physical separation and physical security have to be ensured. The possible problems of insecure wireless LAN configurations have been mentioned above.

Workstations and servers at the home office
In the past, small offices were often connected to their main company or the Internet by dial-up telephone lines. Only a couple of years ago, telephone costs were high and (e.g. in Austria you had to pay approximately 0,08 € even for a local call with a very short connection time). So the organisation was focused on working locally at home, and data were transmitted by bulk transfers.

Today, one can be online all day long for a fixed and small amount of money and "only" the transfer-volume is limited. Therefore client-server-structures (client at home office, server at the company) and enhanced terminal functionality (e.g. X-Window, Microsoft Terminal Server, ...) are of increasing interest today.

So the structure and division of server functionality and clients between home-office and company also influence the choice of the Internet provider. In the following we assume a connection that is online permanently, such as those offered by ADSL (asymmetric digital subscriber line) and television cable providers.

Choosing the Internet Service Provider (ISP)
Selecting the right ISP is a critical task for a tele-worker. A description of an entire decision model is beyond the scope of this paper. We concentrate on some criteria only, which are most relevant in this context.

Basically the needs of tele-workers with their SOHO environments at their tele-offices typically are similar to private users, but there are also significant differences (e.g. online-time, see above), as we have pointed out already.

Services. Typically, self-employed tele-workers want to promote themselves on the net. So, on the one hand, email addresses and presence on the web, possibly with a domain name (DNS, [2]) address and virtual web-server of its own, are an absolute necessity. On the other hand, every public service run on a server at the home-office increases the overall security risks (up-to-date example: CodeRed worm and its variants [3], which spread via a security bug in the Microsoft Internet Information Server [4]). Therefore it makes sense to use the ISP for providing e.g. web-space and email functionality, although this functionality is available on a SOHO environment server too. At this point we want to emphasise that this outsourcing of services to the provider is much more than a question of convenience or bandwidth and transfer volume, it is also a crucial security issue.

Charges and pricing models. Although Internet service pri-

ces and pricing models vary a lot, there are often quantity limits and pricing per megabyte, especially for professional use. However, ISPs usually forbid home-users to make their own services available. (See section "Services" above.) One reason is to encourage the client to make use of ISP value added services, which makes changing to another provider cumbersome and not worthwhile.

In our context, however, that means: if the ISP really disabled all the well-known service ports, downloading data from a tele-office to the company (see section "Access from company to home-office") would become complicated.

IP address assignment. Administration tasks are easier to manage if the ISP provides the tele-worker with one (or several) *fixed* IP address(es).

Bandwidth. The maximum upstream speed is often much more limited than the downstream speed. Because this fact does not influence normal private use - private persons tend to download rather to upload - it is sometimes forgotten when considering the necessary bandwidth for commercial work.

Availability. This is very important for professional use, even for SOHO tele-working environments. Therefore, besides carefully selecting the ISP based on the quality of service, it also makes sense to plan a backup solution. (See next section for more details.)

Adding standard PTT-services to increase availability.
Almost every tele-worker already has a standard telephone and a modem or ISDN-adapter (ISDN = integrated services digital network) at home. Especially if the ISP and the PTT-provider use different cable systems, the old and available communication hardware should be integrated into the new concept as a simple and cheap backup line.

Increasing security by firewalls.
In fact almost every company that supports tele-workers is protected (at least) by a firewall. The special attention that sensitive company data requires should also be given to the tele-offices. We presume that this viewpoint is very common and so do not elaborate it further.

It is not the intention of this paper to discuss additional security requirements for tele-offices, such as virus-scanners, configuration of web-browsers, securing workstations and servers or logging, and so on. Anyhow, we should keep in mind that a firewall is only one step towards a comprehensive security policy.

Use of a dedicated special system "appliance" as firewall.
We prefer to use a *real bastion station* as a firewall. This means, for instance, that the firewall system itself only provides functions that are absolutely necessary to act as firewall and no other software should be installed on the same system. It is hard to push through this principle, because tele-workers often tend to use their server(s) to the full, installing many different services on a single machine. This practice may make sense to some extent, because servers at a tele-office often have a low utilisation rate. Nevertheless, installing multiple services on the bastion station weakens security. Strict separation between firewall and other IT functionality at the tele-office also allows outsourcing of administration responsibility (tele-worker / contracting company / other outsourcer).

Installation of a dedicated security appliance makes the decision/usage independent from the operating system platform(s) used in a tele-office or supported by a contracting company. And security appliances from professional suppliers are trustworthy for most companies.

Also, from a psychological point of view, it is a good idea to use a dedicated system as a "network security appliance". Standard users will accept it as a "black box". And IT specialists cannot or will not install additional software that could compromise security on this system (because it is not a general computer).

Often home-offices cause space restrictions. A dedicated system needs less room than a standard computer. It usually does not include a fan or a hard disk and therefore does not produce noise. In addition, the power consumption is lower.

Encryption issues (VPN)
For security reasons, any communication between tele-worker and company must be encrypted. To ensure encryption and authentication, the firewall has to establish a VPN (=virtual private network [5]). In our experience, we find it best not to trust encryption software for certain communication channels (such as SSL for Web-access or SMIME for securing emails). These applications do a good job, but only a firewall can ensure that *all* traffic to the contracting company is secured. It frees both the tele-worker and the employee to consider encryption every time a new application is installed.

In the section above, we explained why we prefer a dedicated firewall in the home-office. And if there is already a firewall installed, it makes sense to use it as VPN endpoint too.

In order to be compatible (as far as possible) with current and future VPN security solutions, the selection of VPN standards based on IPSec [5] and IKE (=Internet Key Exchange [5]) is a reasonable decision.

CASE STUDY IN DETAIL

As a matter of fact, almost every company network has its own history. Therefore, we start with a description of the pre-given IT network structure, which is the basis for the case study carried out at FIM.

The following "equations" apply:
- network at the FIM-institute :=: company's network
- tele-offices :=: private / home (SOHO) offices of members of the institute or place of work of contractors and students engaged in industry joint research projects.

Given IT infrastructure
- The main network at FIM is located behind a NAI

Gauntlet 5.5 firewall [6] running on Windows NT (C-FW). This international version of the NAI firewall in use does not support VPN. For financial reasons, plans to upgrade the firewall or changing the system (e.g. Checkpoint FW-1 or NG [7]) are not of current concern.

- Additionally, for consistency reasons, some of the FIM-computers are connected directly to the university network (UNI).
- LABs for hands-on sessions are located in a dedicated network segment.
- Tele-offices consist of one or several workstations (WS) and may also include servers. They connect via RAS (=Remote Access Services [8]) or small ISDN dial-up routers.
- Because the network structure at the FIM is straightforward, IP-routing is based on static routing only.

Figure 4 shows this schema simplified, with one tele-office only, which uses the institute (FIM) and therefore the University infrastructure as ISP. Strict restrictions imposed by campus network policy prohibit further expansion of this structure. So in order to connect staff-members' and free-lancers' home offices, we had to look for an ISP.

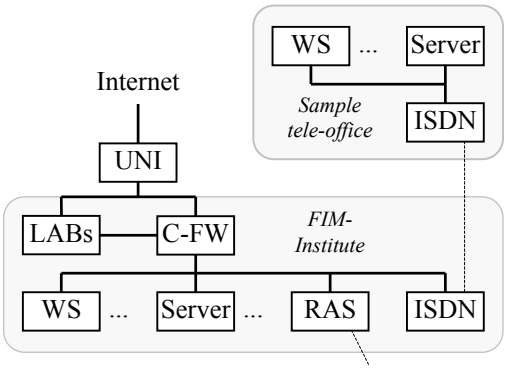

Fig. 4. Existing infrastructure

Internet Provider

Selecting the ISP for the tele-offices was a relatively simple task. We looked for a cheap business solution that provides fixed IP addresses. Prior traffic measurements showed that the maximum transfer rate provided (downstream *and* upstream) is sufficient. The transfer volume per month also seems large enough for the very near future. (We are aware that transfer volume will increase rapidly.) Based on these considerations, and after gathering information about real transfer speeds and availability from partners, we selected LIWEST [9], which is primarily a television provider here in Linz. The two main packages offered by LIWEST concentrate on private and (small) business use, respectively. See table 1 for more details about the price per month. One-off installation costs are not included.

(part 1 of table 1)	LIWEST Business	LIWEST Private
Mailboxes	5	1 + 4 aliases
downstream	512 kbit/sec.	300 kbit/sec.
upstream	128 kbit/sec.	64 kbit/sec

(part 2 of table 1)	LIWEST Business	LIWEST Private
fixed IP addresses	2-4 (internal network+servers)	1 (only a single PC, no servers)
transfer volume	1 GB	"fair use" agreement
additional MB	~6 Cents	-
domain name	1 included	-
Web-space	10 MB (+ virtual web-server)	10 MB
additional 10 MB Web-space	~10,9 €	-
price per month	~66,86 €	~42,15 €
Compare these prices to standard telephone costs: a daytime local telephone call is typically between 3,6 – 6,20 Cents per minute. A call to an ISP Internet number costs ~2,76 Cents daytime.		

Tab. 1. LIWEST prices (date: 2001-07-31)

Additional hardware and software

The previous section, "Increasing security by firewalls", summarises the arguments and reasons for installing a dedicated firewall system as a real bastion station.

We selected SonicWall firewalls [10] because: (a) the favourable price; (b) we had good experiences with another (bigger) solution based on a Checkpoint Firewall at the headquarters of a company, and SonicWall firewalls at all tele-offices.

We decided to buy the smallest and cheapest version of SonicWall: the "SOHO Tele" and the newer "Tele2". It supports up to 5 internal IP-addresses and does not include a DMZ. All further considerations are based on this decision.

The administration interface of a SonicWall is web-based and therefore absolutely independent of the other software platform used. A SonicWall Tele includes the functionality of (a) a firewall (FW) module with "Stateful Inspection" and NAT (Network Address Translation) and (b) a VPN based on IPSec. If the VPN is used for an address range, SonicWall Tele does not support its firewall functionality for this range. Therefore, in the following figures, SonicWalls are displayed as VPN | FW.

To keep the solution simple to administer and reasonably cheap, we have an additional SonicWall at the institute. This system does not work as a firewall; it just serves as endpoint of the VPNs from/to the tele-offices.

Impact on company (institute) structure

Because of this restriction in functionality mentioned above, the SonicWall in the company, which works as endpoint of the VPN, must be connected to the internal network via the company's firewall (Figure 5a). This allows restricting the access of the tele-offices to internal resources via the company's firewall.

A selection of computers on the company's LAN that are

directly accessible from a tele-office via the VPN tunnel can also be made in the VPN-configuration of the SonicWall at the tele-office. This solution makes sense if a central administration authority administers *all* SonicWalls, which, for example, is true for the FIM-institute. Nevertheless, interleaved work with multiple contracting companies is then restricted. If this does not matter, the structure shown in figure 5b can be chosen too.

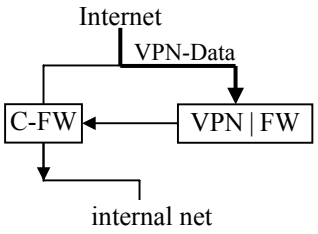

Fig. 5a: Firewall and VPN in parallel

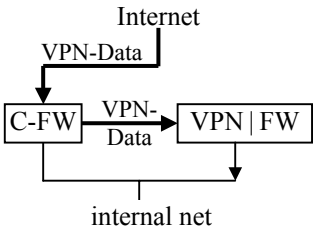

Fig. 5b. Cascading firewall and VPN

Changes in the structure of tele-offices

As shown in the upper part of figure 7, every tele-office is equipped with a small SonicWall. Traffic flows as follows:

- Traffic to special computers or IP-ranges (e.g. at the company's local network) is tunnelled via VPN.
- General access to the Internet works directly via the fire-wall component, which secures the internal network by "Stateful Inspection" and NAT.
- Because NAT is used for Internet access, there is no need to change any of the IP-addresses in the tele-offices.
- The already existing ISDN-router now is used as a backup line. Gateway selection works (a) based on "Dead Gateway Detection" [11] by specifying two gateways in every computer or (b) by simply alternatively turning on/off the SonicWall and ISDN-router, which both have the same internal IP address.

To show that more server functionality from the institute's internal network is used, the server at the home-office in figure 7 is shaded.

Because the VPN and firewall functionality are only available mutually exclusively, computers at a tele-office are normally accessible from the company (here: FIM). A restriction can be configured at the company's firewall C-FW (see figure 5a) or at the VPN-endpoint at the company. This fact has already been discussed, but the other way round, in the section, "Impact on company structure".

Another possible approach is to fully disable several internal IP-addresses by intentionally excluding addresses from the internal address list. These addresses then do not have any access to the outside, and the approach therefore decreases usability. Because this is the only security measure, a tele-worker can carry out at the tele-office, this solution is not suitable for freelancers with higher security requirements.

We do not discuss security issues when the ISDN-router as a backup system is turned on. Security then depends on the functions of the ISDN-routers, which are not described in this paper. Nevertheless, even old ISDN-routers usually support simple filtering functions, such as CLI (=caller line identification), which ensures that only calls from selected telephone numbers are accepted. Encryption may be supported too. We use all these functions at FIM. Additionally, ISDN-routers at the tele-offices are turned on only in case of problems with the ISP service.

Routing issues at the company

Because of the ISDN-based backup system at the tele-offices, the network at FIM has to deal with the following situation: depending on the availability of VPN connections, packets to the same tele-office – which have the same destination IP address - must be routed either via the SonicWall as VPN gateway or via the ISDN router.

Because all routes were statically defined, and because the installation of appropriate routing protocols (particularly on the central firewall) does not make sense, one has to look for another solution. So we implemented a straightforward and simple routing daemon. If PING can reach the external address of the VPN gateway at the tele-office, all traffic from the company to the tele-office is done via the VPN gateway, otherwise the traffic is re-routed to the appropriate ISDN router. The main structure of the routing daemon is shown in figure 6.

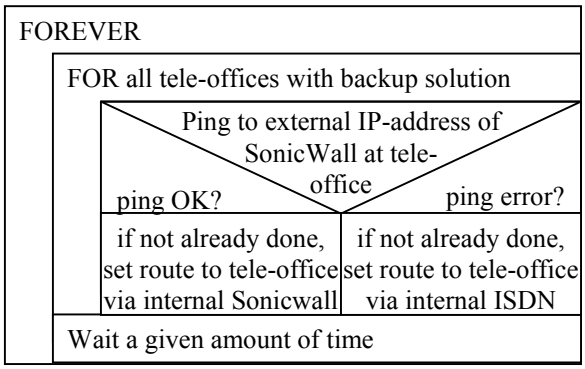

Fig. 6. Nassi Shneiderman diagram of simplified routing

Of course, the simplicity comes at a cost. For example, it is a polling solution and causes permanent small traffic (e.g. 2 pings every 20 minutes). Additionally, ping must be enabled for these addresses at the firewall.

The routing function is implemented as a batch-file (CMD) on Windows NT. It uses the standard commands "ping" or "route" and "sleep" from the NT Workstation or Server Resource Kit [12] for the timing delay. Our complete implementation for multiple tele-offices and with logging and alerting functionality is available for download [13]. The utility AutoExNT from the Resource Kit can be used to start the routing daemon automatically at computer start-up.

Firewalls sometimes modify the IP-stack to obtain additional functions or better throughput, and also perhaps cache information about routes etc. by themselves. In this case, it can happen that a change of route will not cause the firewall to react properly, without making the firewall reload the new configuration or restarting several services. In our example we use the system with the proxies [6] for HTTP+ FTP [2], POP3 [2], SMTP [2], SMB (sever message block) and Telnet [2]. Other proxy configurations,

proxies, patch levels or versions may work differently, so one has to test individually.
It is worth mentioning that this backup solution not only provides the tele-offices with an alternate communication channel to the company (here: FIM), but also would work as a second ISP for the tele-offices. If one wants to have this additional functionality, the firewall rules at C-FW have to be configured accordingly.

CONCLUSION AND SUMMARY

Figure 7 shows an overview of the structure of the case study described.

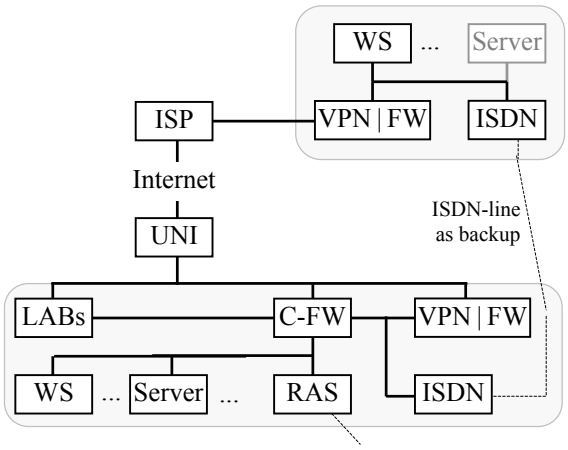

Fig. 7. New infrastructure

Security
Although the range of IP addresses at the tele-offices is rather small (4 / 2 / 1) and is not published as a server-address in DNS or otherwise, there are several queries every day to some well-known ports, for example SMTP, WWW, FTP etc. Nevertheless, some of these scans may originate from the ISP to check that users are not operating (forbidden) services of their own.

Profit of ISDN backup
As dedicated followers of data security and consistent availability of net-access, we insist(ed) on a backup solution, just in case! Therefore we brought in the ISDN backup channel to ensure that we do not have to depend on the availability of the chosen ISP for a set of main services.

Different security requirements
The case study clearly shows that tele-workers who are employees of a company have weaker security requirements than self-employed contractors. Employees typically do not need to protect their tele-office against the company, and there is no need to co-operate with multiple companies.

The association between a company and a self-employed tele-worker falls within the range of an employee doing tele-work and a full B2B (=business to business) solution. The former could (in part) neglect some security requirements of the self-employed contractor while the latter leads to a loss of flexibility. However flexibility should be one of the main benefits when working with a self-employed contractor.

The policy of the FIM institute is to support tele-workers (employees and long-term freelancers) with a small firewall security appliance, which (at least) protects the tele-office from the Internet and secures all traffic between tele-office and the main network. If this solution does not fulfil all security requirements of a freelancer, it is up to her/him to add additional security e.g. by cascading security solutions (for instance a second firewall).

REFERENCES

[1] http://www.theregister.co.uk/content/archive/20920.html
[2] Stevens, W. Richard: TCP/IP Illustrated. Addison-Wesley, Vol. 1, 1994, ISBN 0-201-63346-9
[3] http://www.incidents.org/react/code_red.php and http://www.incidents.org/react/code_redII.php
[4] http://www.microsoft.com/technet/itsolutions/security/topics/codealrt.asp
[5] Kosiur, Dave: Building and managing virtual private networks. Wiley, 1998, ISBN 0-471-29526-4
[6] http://www.pgp.com/products/gauntlet/
[7] http://www.checkpoint.com
[8] http://www.microsoft.com/technet/itsolutions/network
[9] http://www.liwest.at
[10] http://www.sonicwall.com
[11] RFC 816, http://www.freesoft.org/CIE/RFC/1122/56.htm
[12] Microsoft Windows NT Server resource kit. Microsoft, 1996. ISBN 1-57231-344-7
[13] http://www.fim.uni-linz.ac.at/iceta2001

BIOGRAPHIES

Rudolf Hörmanseder received his MSc from the University of Linz 1983. In 1983 he joined the "Forschungsinstitut für Mikroprozessortechnik". Since 1997 he has been a member of the Institute for Information Processing and Microprocessor Technology (FIM). His fields of interest are IT-security, system-administration and operating systems.

Jörg R. Mühlbacher studied mathematics at the University of Vienna and received his PhD in 1969 with a thesis on graph theory. He started his profession as lecturer in computer science (1969-) at the University of Linz and afterwards as professor of computer science (1973-) at the University of Dortmund (Germany). He holds a chair of System Programming the University of Linz (1976-). He is head of the Institute for Information Processing and Microprocessor Technology (FIM) at the University of Linz.