# Personal FireWalls

## … one more step towards comprehensive security

**Dipl.- Ing. Norbert Pohlmann**

Member of the Board

Utimaco Safeware AG

# Table of contents

# 1. Introduction

Most business processes were performed in written form on paper by means of the post or personally in the past. Such processes are nowadays carried out a lot more effectively by use of a commonly used IT infrastructure, the Internet.

Electronic information and data can be integrated into business processes directly and without changing the medium. This trend of reengineering business processes of all kinds corresponds with the general internationalization and globalization. The number of mobile workplaces and telework places is constantly growing, leading to an immense saving of time and money. The necessary link to the Internet, however, implies new dangers, as the latest attack with the virus "I LOVE YOU" has shown dramatically.

It is of vital importance for organizations to define possible threats in order to be able to estimate which attacks could be dangerous and which could be neglected.

Adequate countermeasures help organizations to reduce their vulnerability.

# 2. Risks of connecting to the Internet

Making use of the Internet is an attractive possibility in many respects. One considerable disadvantage, however, is the security aspect. The following risks in particular have to be taken into account:

- Access to valuable information on the computer systems of an organization

  Connecting to the Internet is not a one-way street. Every user of the Internet can generally directly or indirectly access connected computer systems and the resources stored on them (see □ in illustration 1: mobile and telework places or computer systems accessing the Internet without passing the central firewall system).

- Receiving malware (hostile code, damaging programs)

Damaging attacks are often caused by malware (viruses, Trojan horses, worms, etc.). This often results in a reduction of an organization's valuable assets, e.g. due to the destruction of files (see □ in illustration 1). Malware can even be sent within the framework of allowed communication rules over the central firewall system. Malware is typically sent to computer systems as an attachment to mails or within www-documents (Java Applets, Active-X-Controls, and other executables). Active-X-Controls for instance have an unlimited functionality; they can e.g. shut a computer down, delete files or execute other functions that cause damages.

- Cookies and cache

Cookies are stored on a user's PC by the web sites the user went to in order to track the user's activities and to enable the owner of the web site to offer customized products and services. Cookies contain confidential personal information of the user and can also be accessed by others using means of Java or ActiveX, e.g. in order to analyze the user's behavior and use this knowledge for illegal purposes.

Cache are HTML files that are automatically downloaded and stored on a user's PC when accessing a web site. Apart from the waste of storage space on the user's hard disk, the HTML files can also be misused in order to observe the user's behavior (see □ in illustration 1).

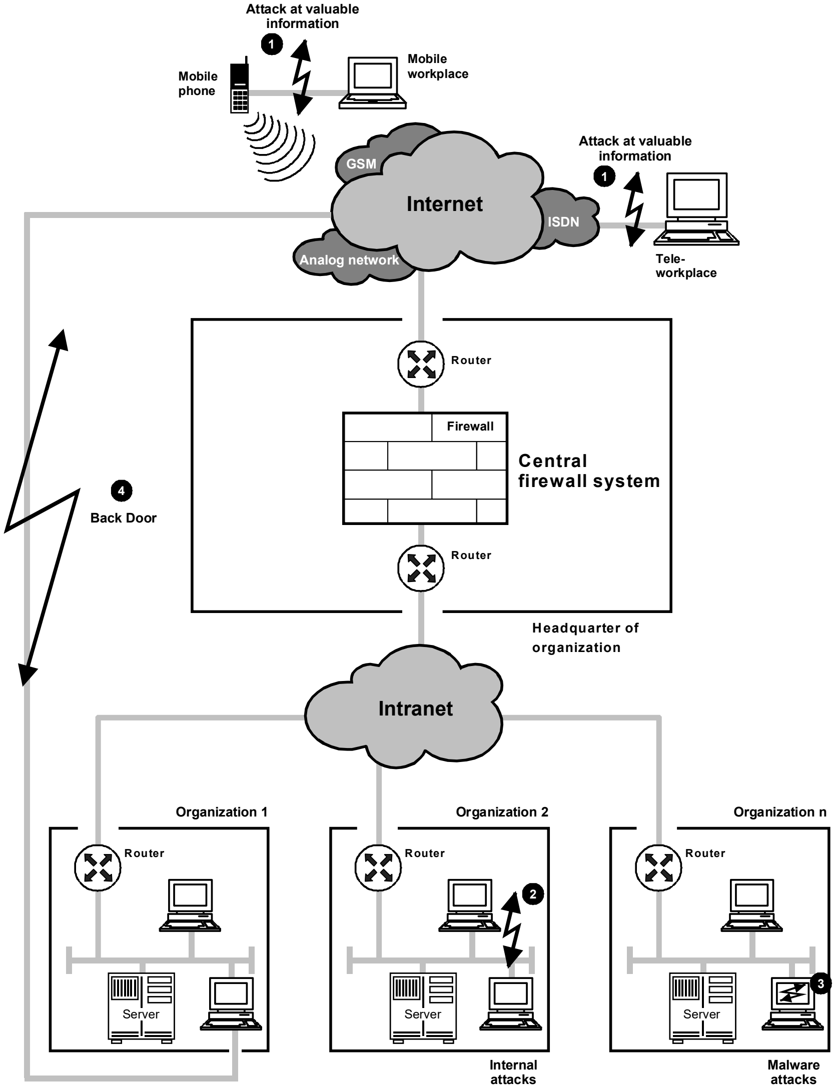

Illustration 1: Risks of connecting to the Internet

Some risks can be easily understood by looking at the "security mechanism" of the conventional security guard of pre-Web ages. The security guard had several jobs; he accepted e.g. packets and controlled whether the addressee was working in the organization, whether the packet was to be accepted at all, etc. Some particularly threatened organizations even have special protection chambers for unpacking packets in which explosives are suspected.

After the addressee had received the packet, he checked if it contained the ordered goods. If so, the goods were integrated into the corresponding business processes.

Such analog security mechanisms are also needed in electronic form.

The typical security mechanisms deployed by organizations are central firewall systems and virus scanners.

# 3. Personal firewall

A personal firewall is intended for use on a desktop PC or notebook having direct access to the Internet, for example, via an Internet provider by dial-up connection (analog network, ISDN, GSM etc.).

These software solutions generally comprise a mixture of packet filter functionality, resource protection (files, ports etc.) and protection against cookies, applets, ActiveX controls etc. [Alad99]. A personal firewall runs in the background.

Simple personal firewall solutions (“light versions”) are administered by the user himself, while enterprise solutions are administered by a central Security Management system so as to implement an enterprise-wide security policy.

Many vendors have announced combinations of personal firewalls with VPN solutions and/or anti-virus solutions [Woel99].

## 3.1. Aim of a personal firewall

The use of personal firewalls is appropriate where it is necessary to counter the design limitations of a central firewall system, for example “backdoors”, “internal attacks” and “malware attacks at data level” [Pohl0001].

The aim of a personal firewall is to close any loopholes that remain in a central firewall system and in known virus scanners, in order to provide full protection to the electronic assets on a PC. For telecommuting and mobile workstations the personal firewall acts as the firewall system when the machine is connected to the Internet.

The personal firewall (also known as desktop firewall, local firewall or distributed firewall) is installed on the PC (notebook or desktop) and protects it against attacks from the network and against threats which can arise in the context of permitted communications through malicious content (malware, mobile codes).

This is achieved not only by strict regimentation of communications on the PC, but also by implementing a secure environment on the sandbox model so as to isolate every application which runs within the operating system. All valuable system resources and files can be shielded against undesirable access through local applications or against malware penetrating the system.

The architecture of a personal firewall is designed in such a way that the security mechanisms are able to restrict access to valuable resources within the application and user context. The security mechanisms are integrated into the operating system in a transparent manner and use their programs, DLLs and kernel device drivers. In this way it is possible to monitor all events and achieve the maximum possible operational security and compatibility.

## 3.2. A personal firewall consists of several components.

The “agent” is the user interface to the personal firewall and displays status information to the user. It monitors particular attacks on the computer environment and resources [Pohl2000].

The “user mode security mechanism” provides higher-level protective measures and protects the runtime environment in a user-oriented fashion.

The “kernel mode security mechanism” provides extended lower-level protective measures and protects the runtime environment. Integration into the kernel level enables maximum control.

The “remote control module” enables the security policy of an organization to be implemented easily via a central Security Management function.

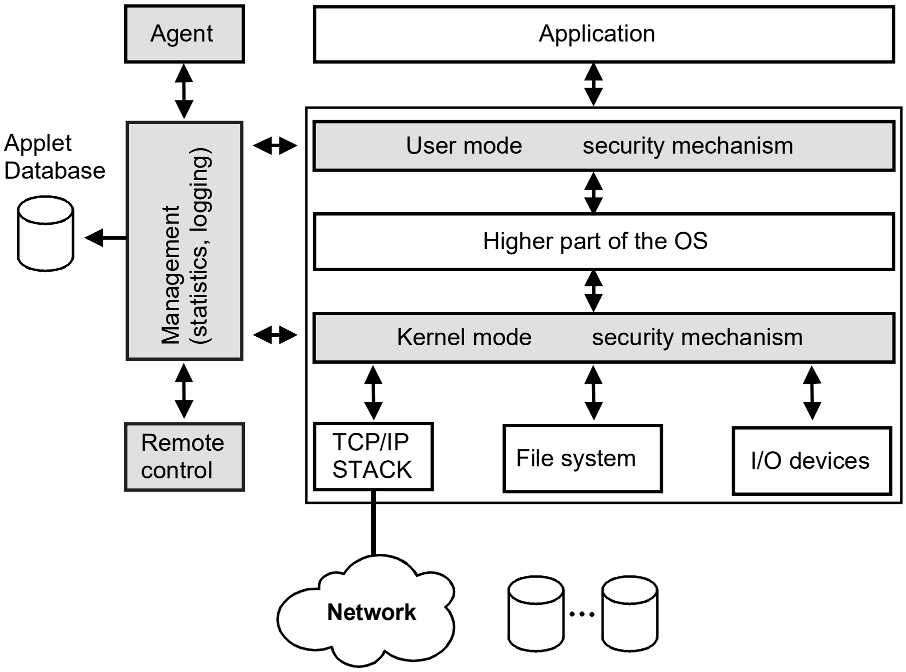

Illustration 2: Architecture of a personal firewall

In the Management Module events are analyzed and logged and statistics are calculated. Cache and cookie management functions that enable usage to be directed and controlled are also typically implemented in the Management Module.

In the Applet Database references to known malicious applets are stored. With these references it is possible to output additional warnings about incoming active content and to block these applets automatically [Sand00].

A personal firewall can be configured offline or online. If configuration is offline, the personal firewall is configured directly on the PC; if online, configuration is controlled centrally.

## 3.3. Security components of a personal firewall

### Firewall component

The packet filter firewall component interprets the packets and checks whether the data in the corresponding headers of the communication layers complies with the defined rule base. The rules are defined so that only necessary communication is allowed and settings known to pose a security risk are avoided.

## Sandbox model

The sandbox model, which is also defined in Java, is a concept for executing a program (Java applets, ActiveX controls and other executables – see picture) in a controlled fashion and in an isolated area in which the program can run its course without influencing the rest of the system. In this way, a potentially malicious application can only access the system to be protected (including the system and network files, resources and connected devices) if the personal firewall allows this. Thus all the system resources are protected against untrustworthy, unknown or malicious applications in an application- and user-defined environment. With the help of access rights management is possible, for example, to specify with which rights browsers may access files or directories. With a sandbox concept it is also possible for resources to be protected against unknown threats.

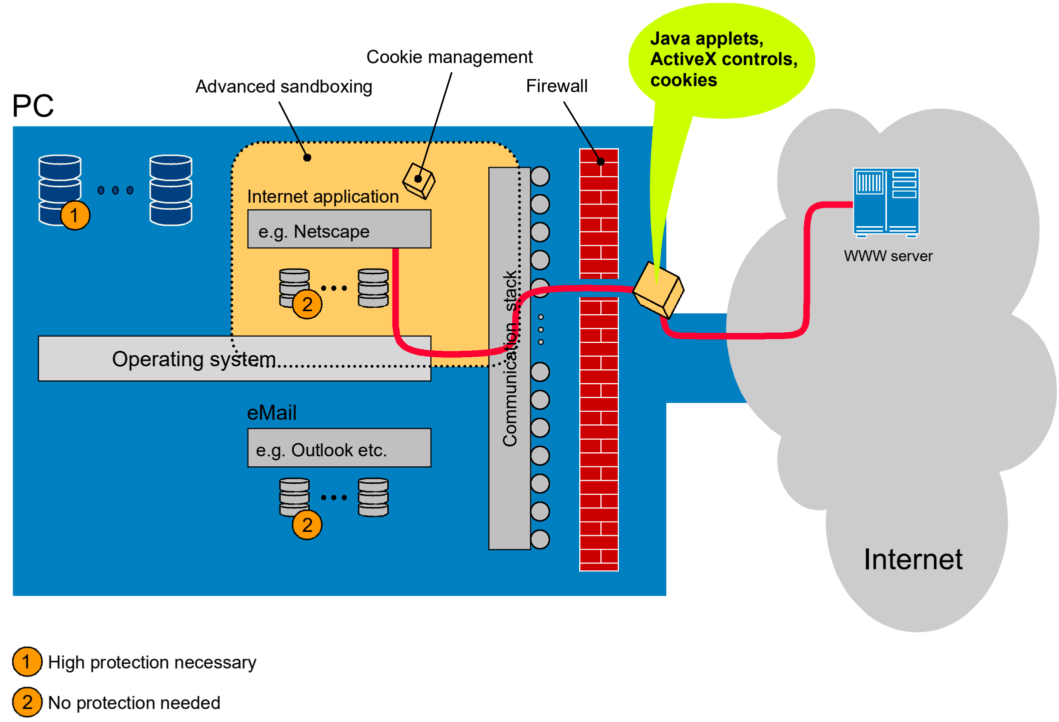

Illustration 3: Protection of data with advanced sandboxing

## Cookie management

With cookie management it is possible to design one's own data protection program. This determines what should happen with which cookies; e.g., which ones are loaded, which ones are not, should the cookies be deleted immediately or should they be deleted when the firewall system is shut down, the aim being to avoid potential data-damaging attacks.

## Example

A user has a personal firewall system installed. If the user now receives an e-mail with the "I love you" virus as an attachment and seeks to execute this attachment, he is asked whether he really wishes some graphics files to be deleted and to send an e-mail to everyone in his address book (the virus pursues the objective of spreading itself as far and as rapidly as possible). In this way the personal firewall gives the user the opportunity to actively intervene before serious harm is done to his organization.

## Secure environment for digital signatures

Another option is the protection of a signature function. Digital Signature Acts in different countries specify that a digital signature must be executed in a secure environment, with no possibility of attacks from outside. With the personal firewall it is possible to ensure that during signing the firewall shuts out all communications so that no attack can occur. No other processes may access the data being signed, resulting in optimum protection and a secure environment for the signature operation.

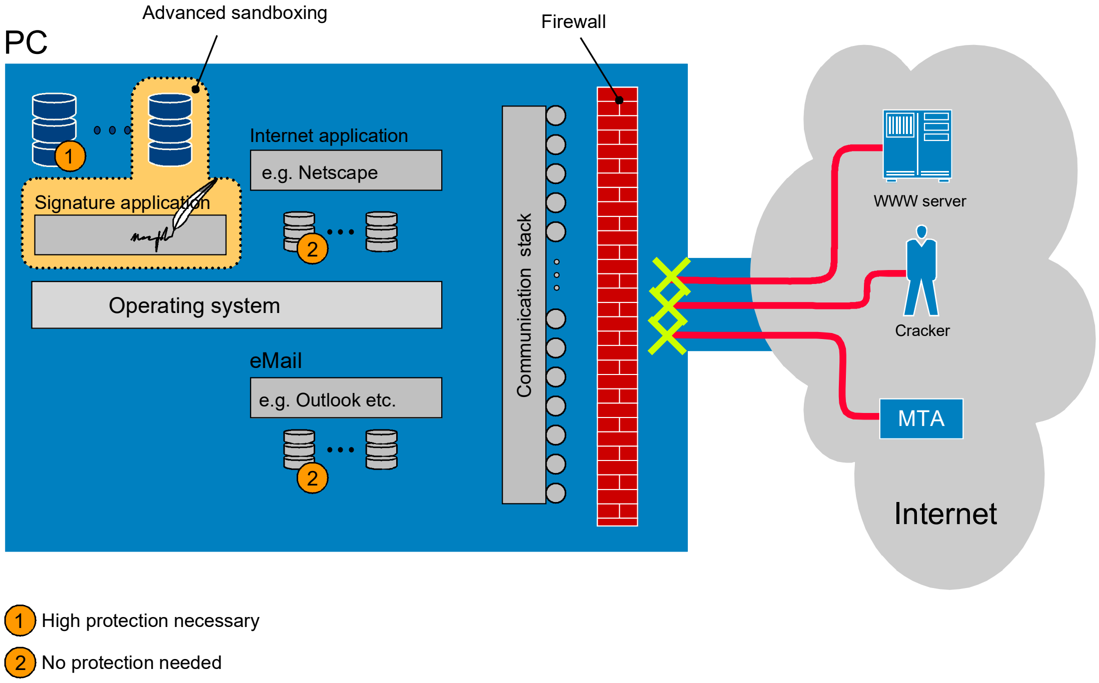

Illustration 4: protection of signature function with advanced sandboxing

## Display, logging and statistics about security-relevant events

The user on the PC is informed when active content (Java applets, ActiveX controls etc.) are installed and/or are started up on the computer system. All suspicious activities are recorded in a logbook and statistical information can be analyzed.

## Practical implementation

To achieve the maximum amount of security, it is recommended to equip computer systems with personal firewalls, in addition to operating a central firewall system and other security mechanisms. In this way comprehensive security is achieved for the resources of an organization. This applies to notebooks in mobile workstations and also to desktop telecommuter workstations and the workstations of the organization itself.

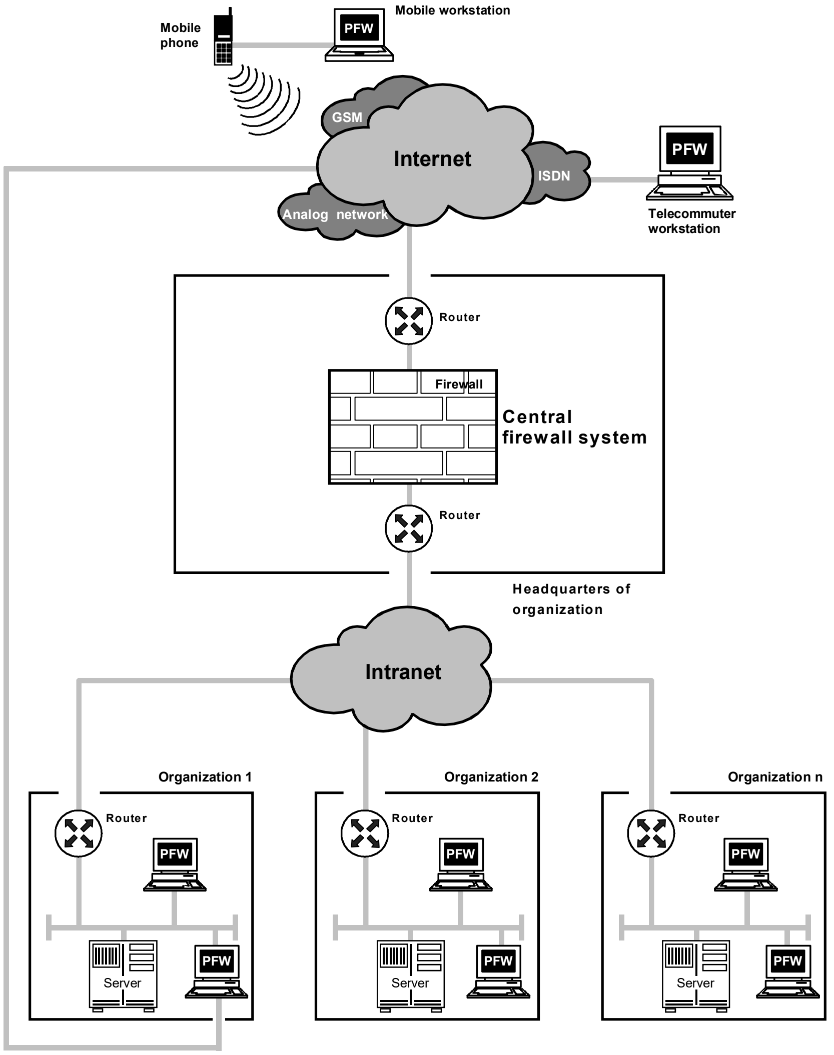

Illustration 5: organization with personal firewalls

## Central administration

If personal firewalls are managed centrally, organizations can implement their own enterprise-wide security policies simply, cost-effectively and securely. The administrator can define access rights with reference to specific applications and/or users, and these rights can then be monitored with the aid of the personal firewall. All the entries necessary for configuration of the personal firewall in the organization are made centrally and disseminated online to the computer systems.

# 4. Summary

With the aid of personal firewalls, it is possible to counteract the increasing vulnerability of electronic assets held on PCs that is associated with increasing use of Internet services.

# 5. Literature

[Alad99] Aladdin. “Safe Internet Connectivity for the Home & Small Office”, White Paper, Aladdin Knowledge Systems, USA , Seattle 1999

[Pohl2001] Norbert Pohlmann: “Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtuel Private Network, Intrution Detection-System, Personal Firewall”, 4. Auflage, MITP-Verlag, Bonn, 2001

[Pohl2000] Norbert Pohlmann: “Dezentrale Firewalls schliessen Lücken”, KES – Kommunikations- und EDV-Sicherheit, SecMedia Verlag, Ingelheim 4/2000

[Sand00] Sandbox: “Protection against Malicious Mobile Code”, White Paper, Sandbox Security AG, Germany, Puchheim, 2000

[Woel99] Woelke von der Brüggen: “Schutz gegen Malicious Mobile Code”, White Paper,
Soft Research Limited, Ireland 1999

# 6. Author

Dipl.-Ing. Norbert Pohlmann

Member of the Board of Utimaco Safeware AG

Chairman of the Board of the TeleTrusT association

Numerous publications, lectures and workshops on topics related to information security document his expertise and commitment in this field.