Personal Firewalls

... Vitamin C für den PC, zur Stärkung der Abwehrkräfte

Autor: **Dipl.-Ing. Norbert Pohlmann**
Member of the Board
Utimaco Safeware AG
☎ 0241-963-1380
🖷 0241-963-1390
E-Mail: norbert.pohlmann@utimaco.de

Inhaltsverzeichnis

1 Einleitung

Die meisten Geschäftsprozesse wurden in der Vergangenheit schriftlich auf Papier mit Hilfe der Post oder persönlich abgewickelt. Solche Abläufe werden heute durch eine gemeinsame IT-Infrastruktur, das Internet, weitaus rationeller gestaltet.

Die elektronischen Informationen und Daten können direkt und ohne Medienbruch in die Businessprozesse einbezogen werden. Dieser Trend des Reengineerings der Businessprozesse in allen Bereichen geht einher mit der Internationalisierung und Globalisierung. Die Anzahl der Mobil- und Heimarbeitsplätze nimmt kontinuierlich zu, das bedeutet auch eine immense Zeit- und Kostenersparnis. Die notwendige Ankopplung an das Internet bringt aber auch neue Gefahren mit sich, wie z.B. der I-LOVE-YOU-Virus gezeigt hat.

Für Organisationen ist es wichtig, die drohenden Gefahren festzustellen, damit eingeschätzt werden kann, welche Angriffe relevant sind und welche vernachlässigt werden können.

Mit Hilfe von geeigneten Gegenmaßnahmen ist eine Organisation in der Lage, die eigene Verwundbarkeit zu reduzieren.

2 Risiken bei der Internet Anbindung

Die Nutzung des Internet ist in vieler Hinsicht attraktiv. Ein gravierender Nachteil ist aber die Sicherheitsfrage, insbesondere sind folgende Risiken zu berücksichtigen:

- Zugriff auf wertvolle Informationen einer Organisation:

  Die Kopplung an das Internet ist keine Einbahnstraße. Alle, die an das Internet angeschlossen sind, können prinzipiell direkt oder indirekt auf das angeschlossene Rechnersystem und die darauf gespeicherten Ressourcen zugreifen (siehe in Abbildung 1: Mobile und Telearbeitsplätze oder Rechnersysteme, die an dem zentralem Firewall-System vorbei auf das Internet zugreifen).

- Empfangen von Malware (Hostile Code, Schadprogramme)

  Ein Angreifer, der eine Organisation schädigen möchte, sendet Malware (Viren, trojanische Pferde, Würmer, etc.). In der Folge erleidet die Organisation eine Reduzierung ihrer Werte, einen Schaden z.B. durch die Zerstörung von Dateien (siehe in Abbildung 1). Das Senden dieser Malware kann auch im Rahmen der erlaubten Kommunikation über das zentrale Firewall-System erfolgen. Typischerweise wird die Malware mit Anhängen an Mails oder innerhalb von WWW-Dokumenten (Java Applets, Active-X-Controls, und andere Executables) an die Rechnersysteme gesandt. Active-X-Controls haben z.B. unbegrenzte Funktionalitäten. Sie können z.B. einen PC herunterfahren, Dateien löschen oder beliebige andere Funktionen ausführen und damit Schaden anrichten.

- Cookies und Cache

  Cookies werden von den Websites, die ein Benutzer besucht hat, auf die PC-Festplatte des Benutzers gespeichert, damit die Aktivitäten des Benutzers zurückzuverfolgen sind und damit der Benutzer langfristig optimal vom Website-Anbieter bedient werden kann. Diese vertraulichen, privaten Informationen können aber auch von Betreibern anderer Websites über Java oder ActiveX abgerufen werden, das Verhalten des Benutzers kann analysiert und dieses Wissen möglicherweise für kriminelle Zwecke genutzt werden.

  Cache sind HTML-Dateien, die beim Zugriff auf eine Website automatisch heruntergeladen und auf dem Rechner des Benutzers gespeichert werden. Neben der Platzverschwendung auf der Festplatte können die HTML-Dateien zur Überwachung des Verhaltens des Benutzers missbraucht werden (siehe in Abbildung 1).

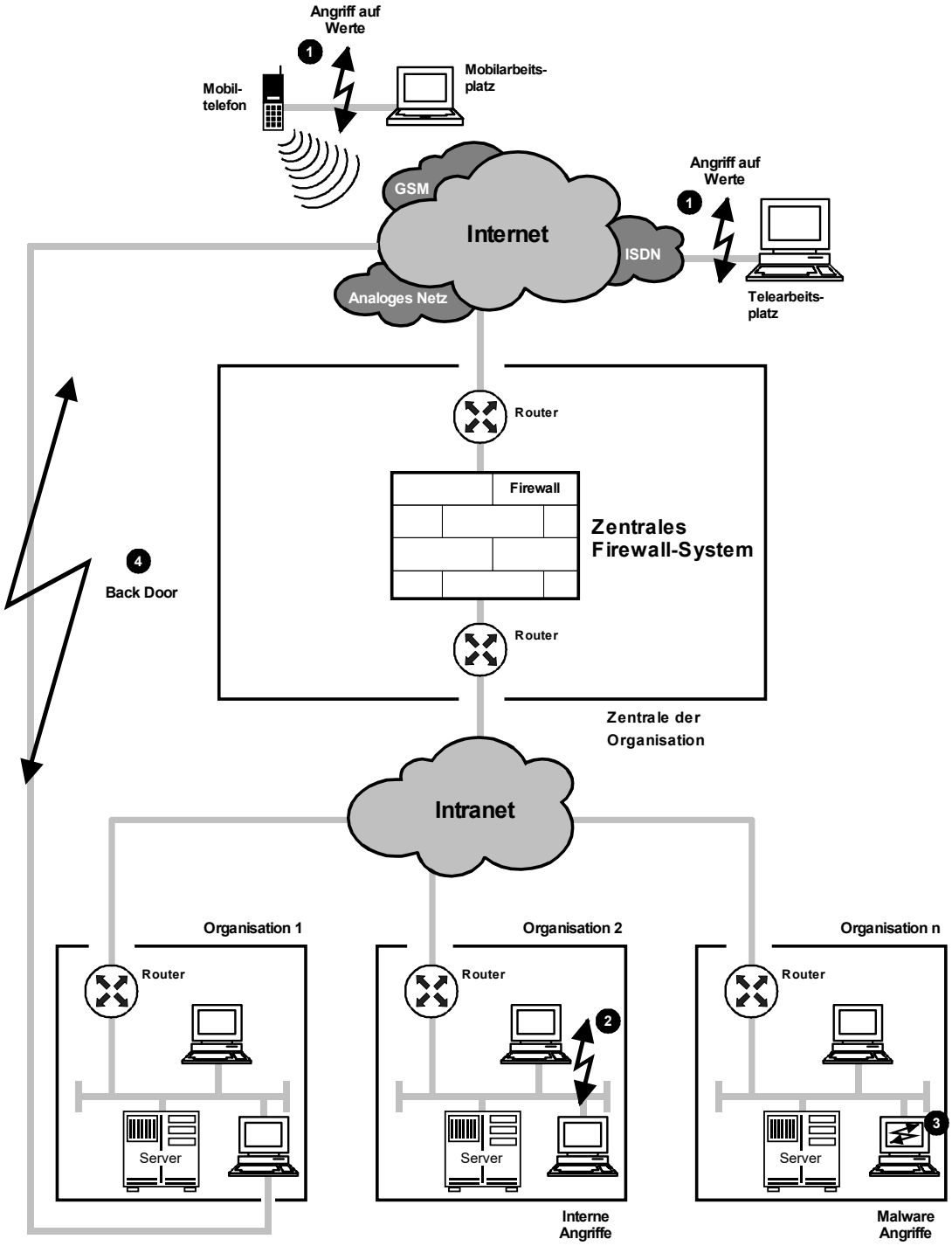

Bild 1: Risiken bei der Internet Anbindung

Trotz der vielfältigen Gefahren sollten oder müssen Unternehmen die Chancen der Internetanbindung nutzen. Zur Verdeutlichung der Situation mag folgenden Analogie dienen:

Angesichts einer grassierenden Grippewelle oder anhaltend schlechten Wetters stehen jedem Einzelnen verschiedene Verhaltensweisen zur Verfügung. Im Schutze des eigenen Hauses zu bleiben, vor die Tür zu gehen und sich ungeschützt dem Risiko der Ansteckung aussetzen oder sich mit viel Vitamin C zu versorgen, um so die Steigerung der Abwehrkräfte zu erzielen.

Die letztgenannte Variante ermöglicht die Freiheit dorthin zu gehen, wohin man will und reduziert die Möglichkeit der Infektion mit Viren.

Die Personal FireWall ist ein dem Vitamin C vergleichbares Schutzschild für den PC und stellt eine sinnvolle Ergänzung zu anderen Sicherheitsmechanismen für Unternehmen und Organisationen dar.

Typischerweise schützen sich Organisationen mit den Sicherheitsmechanismen des zentralen Firewall-Systems und mit Virenscannern.

Zentrales Firewall-System

Ein zentrales Firewall-System ist ein außergewöhnlich effektiver Sicherheitsmechanismus zum Schutz von Netzen. Das zentrale Firewall-System analysiert die Kommunikationsdaten und kontrolliert die Kommunikationsbeziehungen sowie die Kommunikationspartner. Außerdem reglementieren die Sicherheitsdienste eines zentralen Firewall-Systems die Kommunikation gemäß einer organisationsspezifischen Sicherheitspolitik, kontrollieren alle sicherheitsrelevanten Ereignisse und alarmieren bei Verstößen den Security Administrator. Ein zentrales Firewall-System stellt den Common-Point-of-Trust zwischen unterschiedlichen Netzen dar. Die Idee eines zentralen Firewall-Systems besteht darin, nur einen Weg vom zu schützenden in das ungeschützte Netz und umgekehrt zu gestatten und diesen einen Zugang zuverlässig und effektiv zu kontrollieren /Pohl00/.

Es gibt aber auch konzeptionelle Grenzen eines zentralen Firewall-Systems, denen mit anderen technischen oder auch nicht-technischen Sicherheitsmechanismen entgegengewirkt werden muss.

Back Door

Konzeptionelle Grenzen eines zentralen Firewall-Systems beruhen in erster Linie auf sogenannten Hintertüren(back doors). Da das Firewall-System nur Kommunikationsverbindungen schützt, die über das Firewall-System geleitet werden, greift dieser Schutz naturgemäß nicht, wenn Kommunikationsübergänge auch am Firewall-System vorbei möglich sind. In Abbildung 2, , greift z.B. ein Benutzer über die Telefonanlage und einen Internetprovider an dem zentralen Firewall-System vorbei ins Internet.

Interne Angriffe

Ein zentrales Firewall-System bietet Sicherheitsdienste zur Abschirmung gegen das unsichere Netz oder zur Kontrolle der Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz. Das zentrale Firewall-System allein bietet keinen Schutz vor internen Angriffen (siehe in der Abbildung).

Malware-Angriffe auf Datenebene:
Eine zentrales Firewall-System ist ursprünglich nicht in der Lage, im Bereich der erlaubten Kommunikation Angriffe auf der Datenebene zu erkennen. Dazu gehören: Angriffe durch das Senden von Malware wie E-Mail-Attachments, Downloads vom Web, Java Applets und Active-X-Controls (siehe in der Abbildung).

Virenscanner

Zur Erkennung von Viren gibt es sogenannte Virenscanner, die zentral oder auf einzelnen Rechnersystemen nach bekannten Viren suchen. Falls in einer Datei ein Virus erkannt wurde, zeigen sie dieses sicherheitsrelevante Ereignis an.

Auch bei Virenscannern gibt es konzeptionelle Grenzen.

Das generelle Problem bei der Virenerkennung ist die mangelnde Aktualität der Programme. Zu der Vielzahl bestehender Viren kommen praktisch täglich neue hinzu, der Virenscanner kann die Neuentwicklungen nicht erkennen. Folge: Es ist kein hundertprozentiger Schutz vor Viren gegeben. Das Problem steigt bei der Datenübertragung, hier ist die Erkennungsrate von Viren noch geringer.

Wird der Virenscanner zentral eingesetzt, müssen komprimierte Daten immer noch zuerst dekomprimiert werden, um geprüft zu werden. Verschlüsselte Daten können gar nicht geprüft werden.

Virenscanner finden nur Viren, die sie bereits kennen. Ein Virenscanner kann nicht „ausprobieren“, ob eine Datei mit einem Virus etwas Schädliches tut.

3 Personal FireWall

Ziel einer Personal FireWall ist es, die Lücken zu schließen, die bei einem zentralen Firewall-System und bei den bekannten Virenscannern noch vorhanden sind, damit die elektronischen Werte auf einem PC umfassend geschützt sind.

Die Personal FireWall (auch Desktop-Firewall, dezentrale Firewall oder distributed Firewall genannt) ist auf dem PC (Notebook oder Desktop) installiert und schützt ihn vor Zugriffen aus dem Netz und Bedrohungen, die im Rahmen der erlaubten Kommunikation durch bösartige Inhalte gesendeter Daten (Malware, Mobile Codes) entstehen können.

Dazu wird neben der Reglementierung der Kommunikation auf dem PC eine sichere Umgebung nach dem Sandbox-Modell realisiert um jede Anwendung, die innerhalb des Betriebssystem läuft, zu isolieren. Alle schützenswerten Systemressourcen und Dateien können gegen unerwünschte Zugriffe durch lokale Applikationen oder Malware, die in das System eindringen, abgeschirmt werden.

Die Architektur einer Personal FireWall ist so aufgebaut, dass die Sicherheitsmechanismen in der Lage sind, den Zugriff auf schützenswerte Ressourcen innerhalb des Anwendungs- und Benutzerkontextes zu beschränken. Die Sicherheitsmechanismen sind transparent in das Betriebssystem eingebunden und nutzen deren Programme, DLLs und Kernel-Gerätetreiber. Somit können alle Ereignisse überwacht und ein Maximum an Betriebssicherheit und Kompatibilität erreicht werden (siehe Bild 2).

Eine Personal FireWall besteht aus mehreren Komponenten.

Der „Agent“ ist die Benutzerschnittstelle zur Personal FireWall und zeigt dem Benutzer Statusinformationen an. Er überwacht bestimmte Zugriffe auf die Rechnerumgebung und die Ressourcen.

Der „User Mode Security Mechanism“ bietet Schutzmaßnahmen auf höherer Ebene und schützt die Laufzeitumgebung benutzerorientiert.

Der „Kernel Mode Security Mechanism“ bietet erweiterte Schutzmaßnahmen auf niedriger Ebene und schützt die Laufzeitumgebung. Eine Einbindung in die Kernel-Ebene ermöglicht eine maximale Kontrolle.

Das „Remote Control Module“ erlaubt es, über ein zentrales Security Management die Sicherheitspolitik einer Organisation einfach umzusetzen.

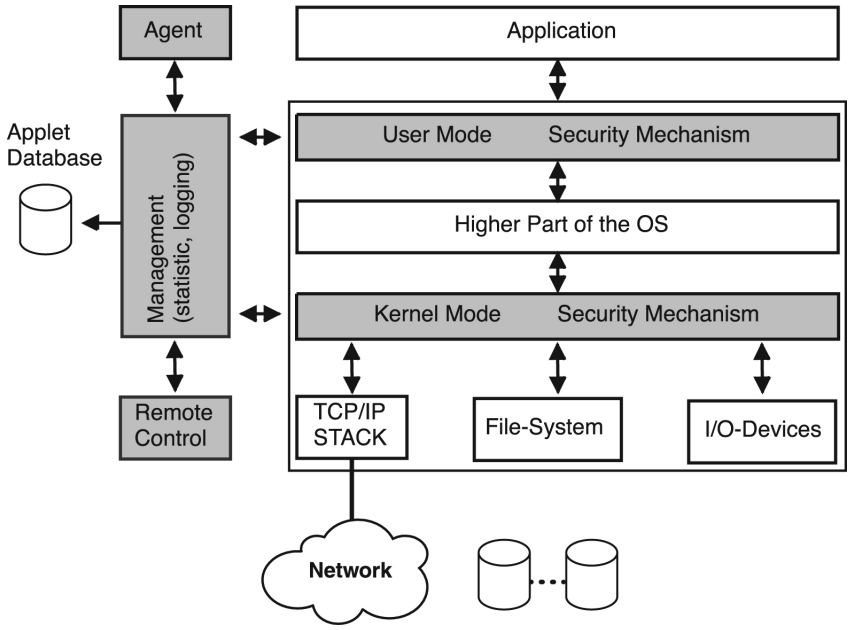

Bild 2: Architektur einer Personal FireWall

Im „Management Module“ werden die Ereignisse analysiert, protokolliert und Statistiken berechnet. Außerdem ist im Management Module typischerweise eine Cache- und Cookie-Verwaltung realisiert, mit deren Hilfe die Benutzung gesteuert und kontrolliert werden kann.

In der „Applet Database“ sind Referenzen von bekannten bösartigen Applets gespeichert. Mit diesen Referenzen ist es möglich, zusätzliche Warnungen über eingehende aktive Inhalte auszugeben oder diese Applets automatisch zu blockieren.

Eine Personal FireWall kann offline oder online konfiguriert werden. Bei offline wird die Personal FireWall direkt am PC konfiguriert, bei online wird die Konfigurierung zentral gesteuert.

Sicherheitskomponenten einer Personal FireWall

Firewallkomponente

Die Firewallkomponente Packet Filter interpretiert die Pakete und verifiziert, ob die Daten in den entsprechenden Headern der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen vermieden werden.

Hier können auf den verschiedenen Kommunikationsebenen unterschiedliche Überprüfungen durchgeführt werden.

- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokolltyp kontrolliert.
- Auf Netzwerkebene wird je nach Protokoll überprüft:
  - IP-Protokoll: z. B. die Ziel- und die Quell-Adresse und das verwendete Schicht-4-Protokoll, aber auch Optionsfeld und Flags
  - ICMP: die ICMP-Kommandos
  - IPX-Protokoll: z. B. Network/Node
  - OSI-Protokoll: die OSI-Netzwerkadresse
- Auf Transportebene findet
  - bei UDP/TCP z. B. eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt (hierüber werden die Dienste wie FTP, Telnet, HTTP - definiert);
  - bei TCP findet z. B. zusätzlich eine Überprüfung der Richtung des Verbindungsaufbaus statt.
- Zusätzlich kann überprüft werden, ob der Zugriff über den Packet Filter in einem definierten Zeitraum durchgeführt wird (zum Beispiel montags bis freitags von 7 Uhr bis 19 Uhr, samstags von 7 bis 13 Uhr, sonntags nicht).

Die entsprechenden Prüfinformationen werden dem Regelwerk entnommen und mit den Analyse-Ergebnissen verglichen.

Sandbox-Modell

Das Sandbox-Modell, das auch in Java definiert ist, ist ein Konzept, das Programme (Java Applets, Active-X-Controls und andere Executables) in einem abgeschlossenen Bereich kontrolliert zur Ausführung bringt, in dem sie beliebig agieren können, ohne den Rest des Systems zu beeinflussen. Auf diese Weise kann eine potentiell bösartige Anwendung nur dann auf das zu schützende System zugreifen (einschließlich der System- und Netzdateien, Ressourcen und verbundenen Geräte), wenn die Personal FireWall dies zulässt. Hierdurch werden in einer anwendungs- und benutzerdefinierten Umgebung alle Systemressourcen vor nicht vertraulichen, unbekannten oder bösartigen Applikationen geschützt. Mit Hilfe der Rechteverwaltung kann z.B. definiert werden, mit welchen Rechten die Browser auf Dateien oder Verzeichnisse zugreifen können. Mit Hilfe des Sandbox Konzeptes können die Ressourcen auch vor unbekannten Bedrohungen geschützt werde.

Darstellung, Protokollierung und Statistiken über sicherheitsrelevante Ereignisse

Der Benutzer am PC wird informiert, wenn aktive Inhalte (Java Applets, ActiveX-Controls, usw.) installiert und/oder auf dem Rechnersystem gestartet werden. In einem Logbuch werden alle verdächtigen Aktivitäten festgehalten. Über Statistikinformation können Auswertungen durchgeführt werden.

Beispiel eines Ablaufes

Auf dem Rechnersystem eine Benutzers ist eine Personal FireWall installiert. Wenn der Benutzer nun eine E-Mail mit dem I-LOVE-YOU-Virus als Anhang empfangen und diesen Anhang zur Ausführung bringen würde, würde er gefragt werden, ob er wirklich möchte, dass Bilddateien gelöscht werden und eine E-Mail an alle, die in seinem Adressverzeichnis stehen, gesendet wird (das Programm verfolgt damit das Ziel, den Virus so weit und schnell wie möglich zu verbreiten). Mit der Personal FireWall hat der Benutzer also aktiv die Möglichkeit, großen Schaden für seine Organisation zu verhindern.

Eben wie Vitamin C für den PC.

4 Praktische Realisierung

Um ein Höchstmaß an Sicherheit zu erreichen, ist es empfehlenswert, die Rechnersysteme zusätzlich zum Betrieb eines zentralen Firewall-Systems und zum Einsatz von Virenscannern mit Personal FireWall auszustatten, um eine umfangreiche Sicherheit für die Ressourcen, die Werte einer Organisation zu erreichen. Dies gilt sowohl für die Notebooks der mobilen Arbeitsplätze als auch für die Desktop Telearbeitsplätze und die Arbeitsplätze in der Organisation selber.

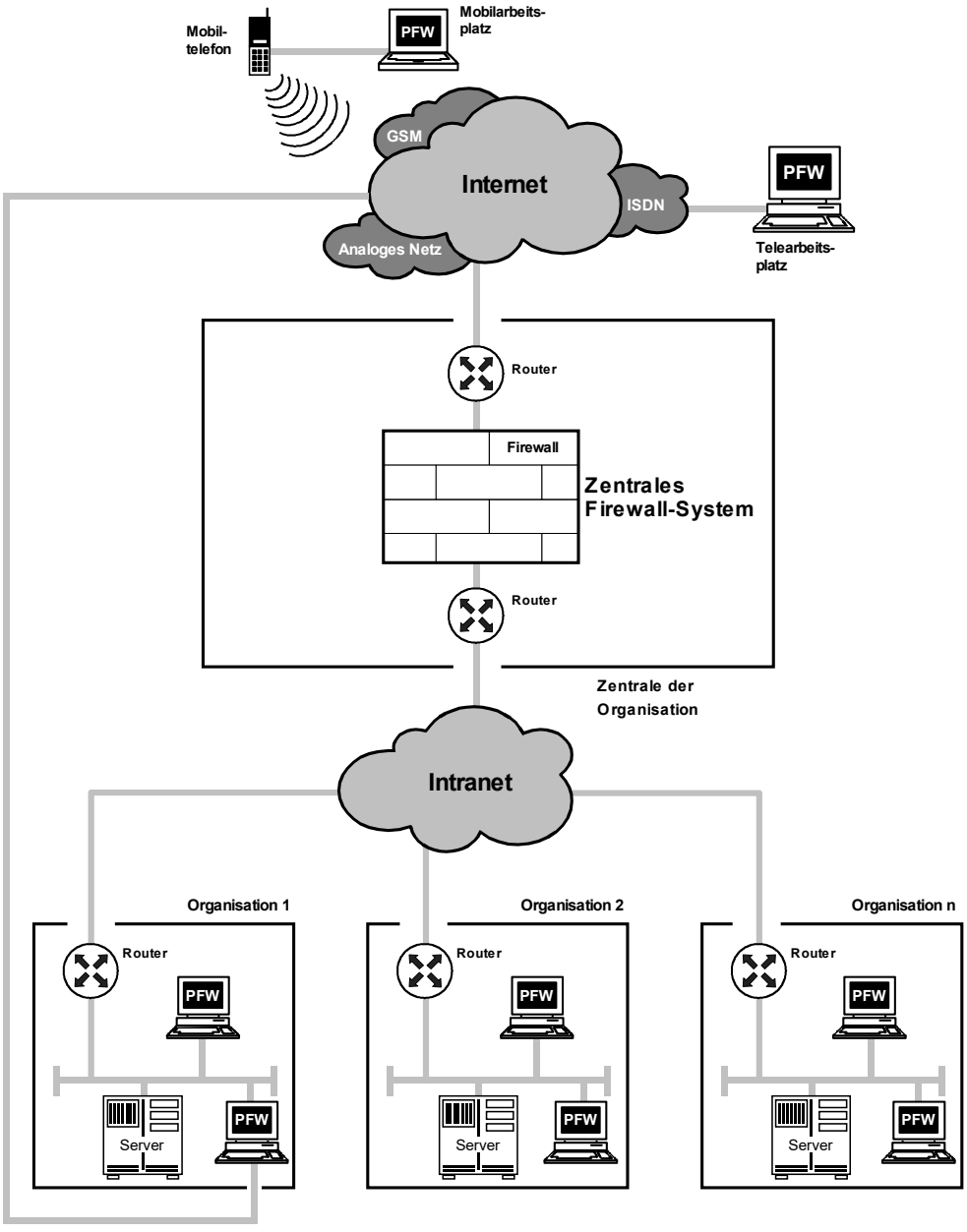

Bild 2: Organisation mit Personal FireWalls

Zentrale Verwaltung

Mit Hilfe der zentralen Verwaltung der Personal FireWall sind Organisationen in der Lage, die eigene Sicherheitspolitik organisationsweit einfach, kostengünstig und sicher umzusetzen. Der Administrator kann anwendungs- und/oder benutzerorientiert die Rechte definieren, die mit Hilfe der Personal FireWall überwacht werden. Alle notwendigen Eintragungen zur Konfigurierung der Personal FireWall in der Organisation werden zentral durchgeführt und online auf die Rechnersysteme verteilt.

Ein weiterer wichtiger Aspekt für die praktische Realisierung ist die enge Verknüpfung von anderen Sicherheitsmechanismen (zentrales Firewall-System, Virenscanner, Festplatten- und/oder Dateiverschlüsselung), damit eine umfassende Sicherheitslösung für die Organisation lückenlos betrieben werden kann.

5 Überblick der Funktionalitäten einiger am Markt verfügbarer Personal Firewalls

In der folgenden Tabelle werden einige am Markt verfügbare Personal FireWalls mit ihren Features dargestellt.

	Conseal PC Firewall	**eSafe Protect**	**Norton Internet Security 2000**	**Sphinx Desktop Firewall**	**SafeGuard Personal FireWall**
Version	2.0.4.	2.2.	1.0.138.0	Beta-Version	1.0.
Hersteller	Network Associates	Aladdin	Symantec	Biodata	Utimaco Safeware AG
Web-Adresse	www.nai.com	www.esafe.com	www.symantec.com	www.biodata.de	www.utimaco.de
Einzelpreis	ca. 115 DM	ca. 129 DM	149 DM	ca. 160 Mark	159 Mark
Sprache	Englisch	Englisch / Deutsch	Englisch / Deutsch	Englisch	Deutsch / Englisch

Produkte	**Conseal PC Firewall 1.35**	**Esafe Protect 2.0**	**Guard Dog 1.3**	**PC Secure 1.1**	**SafeGuard® Personal FireWall**
Firma	**Conseal**	**E-Safe**	**Network Associates**	**Software Builders**	**Utimaco Safeware AG**
Betriebssystem	Windows 95/98/NT	Windows 95/98/NT/W2K	Windows 95/98/NT	Windows 95	Windows 95/98/NT/W2K
Firewall Features					
TCP/IP-Paketfilter	ja	ja	ja (eingeschränkt)	ja	ja
Ports	ja	ja (über Portliste)	nein	ja	ja
manuelles Hinzufügen von Ports	ja	ja	nein	ja	ja
IP Adresse	ja	ja	nein	ja	ja
Content Filter	ja	ja	nein (eingeschränkt)	ja	ja
Richtungsangabe der Filterung .	ja	ja	nein	ja	ja
Regelset	ja	ja	nein	ja	ja
ständiger Überwachungsmodus	ja	ja	ja	ja	ja
Zugriffskontrolle auf Systemressourcen	ja	ja	ja	ja	ja
Warnmodus	ja	ja	ja	ja	ja
Verbindung manuell annehmen	ja	ja	ja	ja	ja
Verbindung manuell ablehnen	ja	ja	ja	ja	ja
benutzerdefinierte Reaktion	ja	ja	ja	ja	nein
Zeitsteuerung	ja	ja	nein	nein	nein
Liste kritischer Informationen (z.B. Passwörter, Kreditkarteninformationen)	nein	ja	nein (nur PW-Dateien von Windows)	nein	nein
Upgrade-Möglichkeit zur Netzwerkversion	nein	ja	nein	nein	ja
Logfiles	ja	ja	nein	ja	ja
Java-Applets					
Ablehnen	nein	ja	nein	nein	ja
Annehmen	nein	ja	nein	nein	ja
selektive Annahme	nein	ja	nein	nein	ja
Liste kritischer Applets	nein	ja	nein	nein	ja
ActiveX-Controls					
Ablehnen	nein	ja	nein	nein	ja

Annehmen	nein	ja	nein	nein	ja
selektive Annahme	nein	ja	nein	nein	ja
Liste kritischer Controls	nein	ja	nein	nein	ja
Virenscanner					
Echtzeit-Hintergrund-Scan	nein	ja	nein	nein	ja
Scan-Sets	nein	ja	nein	nein	ja
Scannen von Downloads	nein	ja	nein	nein	nein
Unterstützung gepackter Dateien	nein	ja	nein	nein	nein
Makro-Viren	nein	ja	nein	nein	ja
Mail-Attachments	nein	ja	nein	nein	nein
Updates via Intemet	nein	ja	nein	nein	ja
Sonstiges					
Browser-Cache	nein	ja	k.A.	ja	ja
History	nein	ja	ja	nein	ja
Cookie-Manager	nein	ja	ja	nein	ja
Besonderheiten	umfassende Konfigurations-möglichkeiten	Sandbox für aktive Inhalte	keine	keine	Sandbox um Browser

6 Zusammenfassung

Mit Hilfe der Personal FireWall kann die durch die zunehmende Nutzung der Internet-Dienste zunehmende Verwundbarkeit der elektronischen Werte auf dem PC stark reduziert werden.

7 Literatur

/Pohl00/ Norbert Pohlmann: „Firewall Systeme – Sicherheit für Internet und Intranet; E-Mail-Security, Virtual Private Networks; Intrusion Detection-Systeme“ – 3. Auflage, MITP-Verlag, Bonn, 2000

8 Autor

Vorstandsmitglied der Utimaco Safeware AG

Vorstandsvorsitzender des TeleTrusT e.V.

Zahlreiche Veröffentlichungen, Vorträge und Seminare auf dem Gebiet der Informationssicherheit dokumentieren seine Fachkompetenz und sein Engagement auf diesem Gebiet.