Forschungszentrum Jülich

**Zentralinstitut für Angewandte Mathematik**
**D-52425 Jülich, Tel. (02461) 61-6402**
**Informationszentrum, Tel. (02461) 61-6658**

**Technische Kurzinformation**
FZJ-ZAM-TKI-0354
*J.Meißburger*
16.11.2000

---

# Zur Sicherheit von Windows-PCs im Internet

---

**Inhaltsverzeichnis:**

Einleitung
1. Sicherheits-Patches und Updates

2.1 Benutzeranmeldung
2.2 Die Freigabe von Systemressourcen
2.3 Dienste im LAN

3. Sicherheitsoptionen von Windows-Anwendungen

3.1 Macrovirus-Schutz
3.2 Sicherheitseinstellungen im Internet-Explorer

4. Antiviren-Programme
5. @Guard: Ein Firewall für Internet-PCs

---

## Einleitung

Der Anschluß eines PCs an ein Netzwerk und insbesondere die Arbeit im weltweiten Internet birgt Gefahren, die heute wohl allgemein bekannt und bewußt sind: Ausspähen persönlicher Daten, Kompromittierung des Systems durch Einschleusen von Viren oder Ausführung schädlicher Aktionen durch in Webseiten und Email-Attachments versteckte Programme oder einfach Mißbrauch der Systemressourcen durch Fremde. Das einzelne Endsystem kann sich gegen diese Gefahren im wesentlichen durch folgende Vorkehrungen schützen:

1. Nutzung aktuellster Betriebssystem- und Anwendungsversionen, Einspielen eventuell verfügbarer Sicherheitspatches und regelmäßiges Sichern des Betriebssystems.
2. Aktivierung und Nutzung der systemeigenen Sicherheitskomponenten wie paßwortgeschützte und möglichst verschlüsselte Benutzerauthentisierung sowie Vermeidung "offener", d.h. anonymer Accounts und Shares (ZAM-TKI-0147 und ZAM-TKI-0177).
3. Die korrekte Einstellung der in den Internet-Explorer und in viele makrofähige Applikationen wie etwa MS-Word bereits eingebauten Sicherheitsmechanismen.
4. Die Einrichtung eines Virenschutzprogramms wie beispielsweise "F-Prot" oder "Net Shield" von Network Associates mit umfangreichen Prüfmöglichkeiten für Programmausführung, Email- und File-Download sowie automatisierter Aktualisierung der Virensignaturen und Scanprogramme (ZAM-TKI-0355).
5. Schließlich die Einrichtung eines persönlichen Firewalls wie z.B. @Guard auf dem PC zur detaillierten Kontrolle und Steuerung des gesamten IP-Verkehrs und der Webinhalte (ZAM-TKI-0349 und ZAM-IB-9916 ).

Versucht man, die möglichen Einsatzszenarien eines PCs und alle verfügbaren Sicherheitstechniken detailliert zu beschreiben und

für jeden Einzelfall Empfehlungen auszusprechen, scheitert man sehr schnell an der Komplexität der Aufgabe. Eine Konfiguration, die für die meisten Anwendungen ausreichende Sicherheit bietet und ein komfortables Arbeiten auch im Internet erlaubt, ist dagegen leichter zu erstellen und reduziert das Risiko bei einem bewußten Navigieren im Internet auf ein vertretbares Maß.

Wer das Restrisiko scheut, sollte auf vollständige Verschlüsselung der Daten und der Datenkommunikation setzen. Allerdings schützt auch dies nicht vor möglichem Schaden im Betriebssystem durch aktive Inhalte dubioser Webserver oder durch Email. Auf jeden Fall sollte deshalb jedes System über ein unversehrtes, viren- und fehlerfreies Image-Backup verfügen, mit dessen Hilfe das Laufzeitsystem jederzeit restauriert werden kann (Hierzu ein durchaus lesenswertes Papier von V.Rüdigkeit: "Beim nächsten Boot wird alles gut").

Seite 1

## 1. Sicherheits-Patches und Updates

Das ZAM bietet unter der Adresse http://www.fz-juelich.de/zam/docs/topic/lit-security.html eine Anzahl technischer Dokumentationen zum Thema Netzwerk- und Systemsicherheit an. Wer sich über die neuesten Entwicklungen zum Thema Sicherheit informieren möchte, sollte die Webseiten des "CERT Coordination Center"

http://www.cert.org,

die CERT-Seiten "Sicherheit im DFN" des Deutschen Forschungsnetzes

http://www.cert.dfn.de

oder die Sicherheitsseiten des Herstellers Microsoft

http://www.microsoft.com/security

besuchen. Dort finden sich aktuelle Meldungen zur Sicherheitssituation und häufig auch die Patches zur Beseitigung von Sicherheitslücken ( ftp://ftp.cert.dfn.de/pub ).

Eine Vorauswahl solcher Sicherheitsmeldungen mit zusätzlichen Informationen für JuNet stellt das ZAM unter

news://news.kfa-juelich.de/kfa.zam.security

zur Verfügung. Wer sich automatisch mit Email über aktuelle Sicherheitsmeldungen informieren lassen möchte, kann dies durch eine kurze Mitteilung an r.theisen@fz-juelich.de einrichten.

Seite 1

## 2. Sicherheitsfunktionen des Betriebssystems

Die grundlegenden Sicherheitsfunktionen stützen sich bei Windows wie bei allen anderen modernen Mehrbenutzersystemen auf die Anmeldung des Benutzers im System und im Microsoft-Netzwerk. Damit wird primär der Zugriff auf Ressourcen des lokalen Systems und der anderen Rechner im Netzwerk geregelt. Fast ebenso wichtig für die Sicherheit ist die Konfiguration der Freigabe von Ressourcen im Netzwerk ("Shares" oder "Freigaben") und schließlich die Exposition des Systems im Netz durch Aktivieren netzwerkfähiger Dienste. Hier sollen diese wesentlichen Punkte kurz angesprochen werden:

### 2.1 Benutzeranmeldung

Die Benutzer-Authentisierung bei der lokalen- oder der Netzwerk-Anmeldung auf einem Windows- System bietet bei NT/2k die Möglichkeit, eine echte, benutzerbezogene Zugriffsverwaltung für die Systemressourcen einzurichten. Bei Windows 95/98 dient sie lediglich der Unterstützung benutzerspezifischer Profile und zur Authentisierung für den Zugriff auf Rechner der eigenen Arbeitsgruppe. Da beispielsweise auch die Email-Profile (MAPI) mit den Adreßbüchern, Web-Favoriten und Paßwörtern für den Netzzugang benutzerspezifisch abgespeichert werden, empfiehlt sich unter allen Umständen **die Einrichtung individueller, paßwortgeschützter Accounts** ("Einstellungen - Systemsteuerung - Benutzer"). Es versteht sich von selbst, daß keine trivialen Paßwörter, sondern solche ausreichender Länge, möglichst mit Sonderzeichen und ohne leicht zu erratenden Bezug zur fachlichen oder persönlichen Umgebung gewählt werden sollten.

Auf NT-Systemen kann man darüberhinaus den Zugang für "Gast" (erforderlich z.B. für die anonyme Freigabe von Shares) im Benutzer-Manager mit

"Start - Programme - Verwaltung - Benutzer-Manager"
"Gast selektieren - Benutzer - Eigenschaften - Konto deaktiviert"

deaktivieren und gegebenenfalls auch den wohlbekannten Namen "Administrator" des Systemadministrators mit

"Administrator selektieren - Benutzer - umbenennen"

ändern, um den unerwünschten Zugriff zu den Systemressourcen weiter zu erschweren.

In Verbindung mit einem **BIOS-Paßwort**, das ein unbefugtes Booten des PCs von Festplatte oder Diskette verhindert, und einem **paßwortgeschützten Bildschirmschoner** wird ein gewisses Maß an Sicherheit gegen unberechtigten Zugriff durch Fremde erreicht. Das Einrichten der Paßwörter für Betriebssystem und BIOS geschieht beispielsweise beim ASUS-Board mit Festhalten der <Entf>-Taste beim Booten, Eintragen des Supervisor- und User-Passwords und Setzen der "Security Options: System" im "BIOS Features Setup".

**2.2 Die Freigabe von Systemressourcen**

Alle Windows-Systeme erlauben den Zugriff auf Laufwerke, Ordner und Drucker aus dem Netz durch Freigabe sogenannter "Shares". Je nach Betriebssystem wie etwa Windows-NT oder Installation bestimmter Applikationen wie beispielsweise FrontPage werden solche Freigaben auch automatisch bei der Softwareinstallation eingerichtet. Die Freigabe solcher Shares bedeutet, daß diese von anderen Rechnern im Netz aus sichtbar sind, und daß auf sie aus dem Netz zugegriffen werden kann, wobei die Art des Zugriffs (Lesen, Schreiben) und der zugriffsberechtige Personenkreis (bei Windows NT) noch näher spezifiziert werden können.

Windows-NT gibt generell für administrative Zwecke einige Shares mit nicht modifizierbaren Zugriffsberechtigungen für Festplatten und das Windows-Systemverzeichnis mit Namen wie ADMIN$, C$, D$ ..... frei. Das an den Freigabenamen angehängte Dollarzeichen verhindert, daß diese Freigaben beim "Browsen" der Rechner im Netz angezeigt werden. Dieses Verfahren läßt sich auch für eigene Freigaben einsetzen, die man nicht für andere Rechner sichtbar machen möchte. Einen Überblick über die durch das eigene System freigegebenen Shares kann man sich auf DOS-Ebene mit dem Befehl

```
C:\>net share

Name         Ressource                      Beschreibung

-------------------------------------------------------------------------------
ADMIN$       C:\WINNT                       Remote-Admin
IPC$                                        Remote-IPC
C$           C:\                            Standardfreigabe
D$           D:\                            Standardfreigabe
P$           P:\                            Standardfreigabe
Der Befehl wurde erfolgreich ausgeführt.
```

verschaffen.

Vorsicht ist geboten, falls man von einem Fremdrechner aus einmal auf Shares der eigenen Maschine zugreift. Das Paßwort für den Zugriff wird gespeichert, so daß anschließend auch Fremde selbst nach Trennen der Verbindung erneut und ohne Paßwortangabe auf den Share zugreifen können.

Für die Wahl von Paßwörtern zur Freigabe gelten die gleichen Regeln wie oben. Es ist ein gängiges Verfahren von Hackern, nach freigegebenen Ressourcen auf fremden Rechnern zu suchen und sich durch Probieren häufig benutzter Paßwörter Zugang zu den Daten zu verschaffen. Wer über einen Mechanismus zur IP-Portfilterung verfügt (siehe unten), sollte die für diese NETBIOS-Zugriffe benötigen IP-Ports 137 (nbname), 138 (nbdatagram) und 139 (nbsession) für den Zugang von außen sperren oder zumindest die Zugriffe loggen.

Auf Windows 98 und NT-Systemen vor allem in unstrukturierten Netzen sollte unbedingt die Paßwortverschlüsselung aktiviert sein,

um ein Ausspähen der Paßwörter, die ja häufig auch für den Zugang zu anderen Rechnern benutzt werden, in Klartext verhindern. Die Paßwortverschlüsselung kann über Einträge in der Windows-Registry aktiviert werden. Nähere Informationen zu den Registrierungsschlüsseln für die verschiedenen Windows-Versionen stellt das ZEL unter

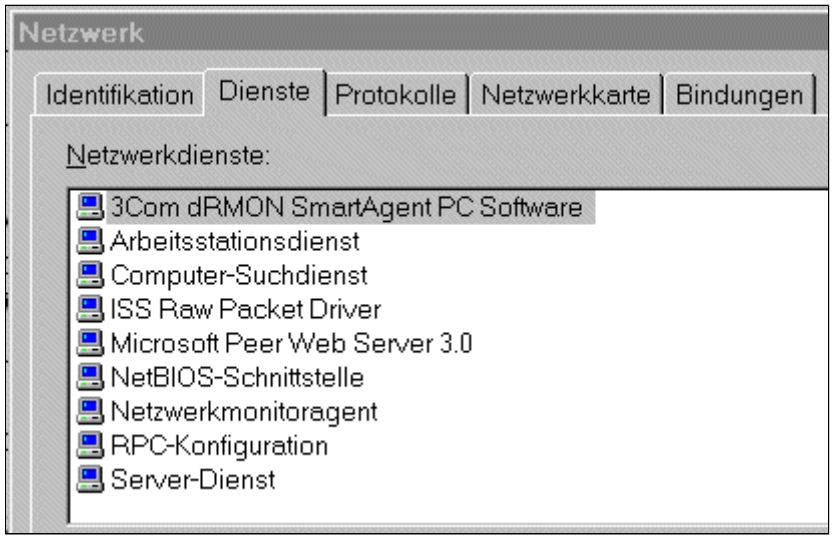
\\zelcds.zel.kfa-juelich.de\public\Samba

zur Verfügung.

Seite 1

**2.3 Dienste im LAN**

Die LAN-Dienste von Windows lassen sich nur unter Windows-NT individuell konfigurieren. Für Windows 95/98 empfiehlt sich für diesen Zweck der Einsatz des persönlichen Firewalls "@Guard". Einen Überblick über die installierten Dienste bei Windows-NT liefert wie im folgenden Beispiel




"Netzwerkumgebung - Rechte Maustaste - Eigenschaften - Dienste"

Die wichtigsten Dienste sind:

- 3Com dRMON SmartAgent PC Software: Zur Fernüberwachung des Ethernetanschlusses mit SNMP
- **Arbeitsstationsdienst**: Erlaubt dem Rechner, als Client im Microsoft-Netzwerk zu arbeiten
- Computersuchdienst: Durchsucht ein Microsoft-Netzwerk nach freigegebenen Ressourcen.
- Microsoft Peer Web Server: Ein einfacher Webserver für das Web-Publishing
- NetBIOS-Schnittstelle: Erlaubt die Ausführung von NETBIOS-Applikationen auf dem Rechner
- Netzwerkmonitoragent: Erlaubt die Fernüberwachung des Rechners
- **RPC-Konfiguration**: Remote Procedure Call, auch lokal benutzt
- Serverdienst: Erlaubt die Freigabe von Druckern und Ordnern

Für Standalone-Rechner, die nur lokal arbeiten und im Internet "surfen" oder Email empfangen wollen, sind nur die markierten Dienste erforderlich. Wer über Shares auf fremde Rechner zugreifen oder selbst Shares freigeben will, benötigt noch den **Computersuchdienst**, die **NetBIOS-Schnittstelle** und den **Server-Dienst**. Man sollte Microsoft-Standarddienste, die man nicht benutzt, besser nicht völlig entfernen, sondern nur in der Systemsteuerung mit

"Start - Einstellungen - Systemsteuerung - Dienste"

deaktivieren, indem man die Startart solcher Dienste von "Automatisch" auf "Manuell" setzt. Dies empfiehlt sich beispielsweise für "Einfache TCP/IP-Dienste", "WWW- und FTP-Veröffentlichungsdienst" und alle "SNMP"-Dienste.

Seite 1

## 3. Sicherheitsoptionen von Windows-Anwendungen

### 3.1 Macrovirus-Schutz

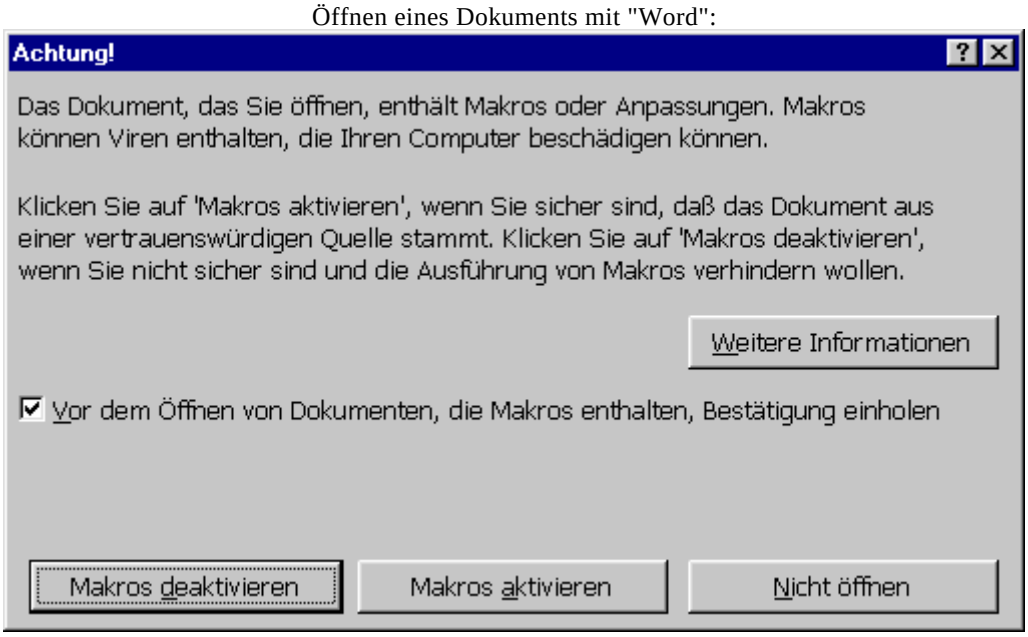
Die meistbenutzen Windows-Anwendungen wie Word, Excel, PowerPoint oder Access unterstützten die Programmierung durch **V**isual **B**asic for **A**pplications (**VBA**) oder durch interaktive Aufzeichnung von Makros. Solche Makros sind Bestandteil des Dokuments und können mit diesem als Datei gespeichert oder als Email verschickt werden (Mail-Attachment). Beim Öffnen eines solchen Dokuments wird das enthaltene Makroprogramm ausgeführt und hat damit Zugriff auf alle Komponenten des Betriebssystems.

Die Windows-Applikationen besitzen deshalb seit längerem einen eingebauten Macrovirenschutz. Er wird in allen Anwendungen durch Starten des Programms und

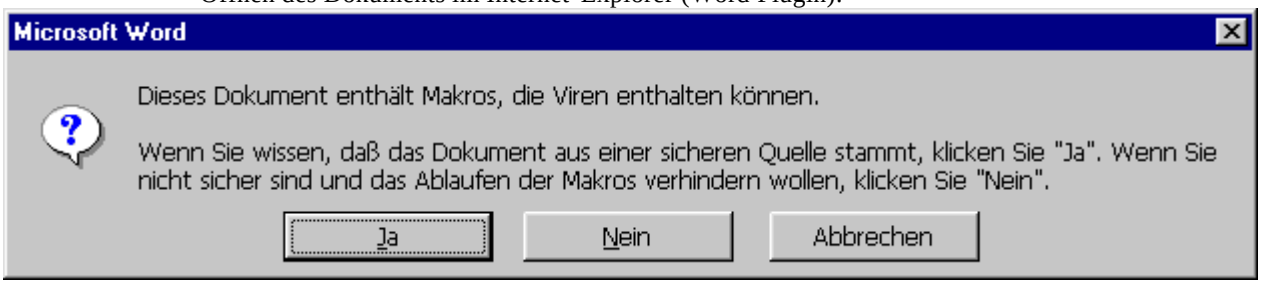
"Extras - Optionen... - Allgemein - ☑ Makrovirus-Schutz "

aktiviert. Er warnt den Benutzer beim Öffnen eines Dokuments, das Macros enthält, vor der Ausführung solcher Macros und bietet in einem Auswahlmenü die Möglichkeit, die Macroausführung zu unterbinden bzw. das Dokument gar nicht erst zu öffnen. Beim Öffnen eines "Word"-Dokuments sieht das beispielsweise beim Öffnen mit Word selbst und beim Öffnen durch Klicken eines Weblinks im Internet-Explorer wie folgt aus:

Öffnen eines Dokuments mit "Word":




Öffnen des Dokuments im Internet-Explorer (Word Plugin):




Vor allem beim Öffnen von Anlagen zu Email-Nachrichten in einem der Windows-Dokumentenformate ist dieser Schutz unbedingt wichtig und sollte nie abgeschaltet werden! Wer durch einen kurzen Test seine Einstellungen für MS-Word testen möchte, kann dieses Dokument öffnen, das ein harmloses Word-Macro mit einer kurzen PopUP-Meldung enthält.

Seite 1

### 3.2 Sicherheitseinstellungen im Internet-Explorer

Die Einstellungen zur Sicherheit des Internet-Explorers V5.x finden sich im Menü

"Extras - Internetoptionen - Sicherheit"

und

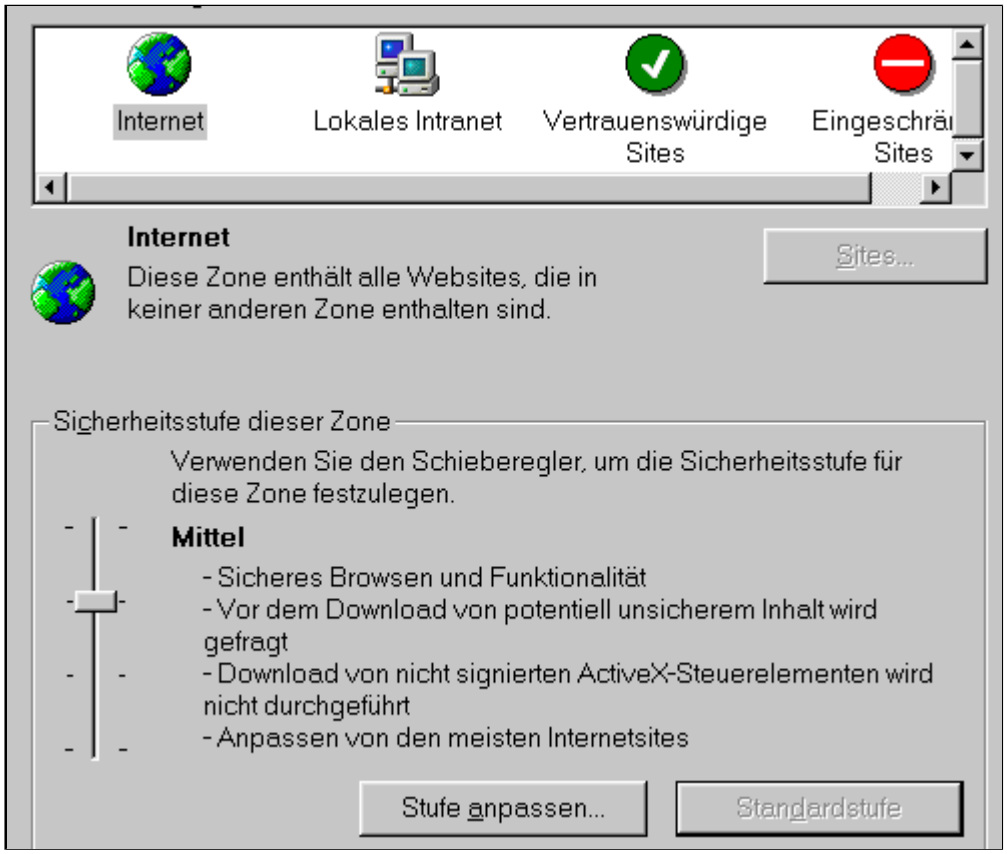
"Extras - Internetoptionen - Erweitert".

Unter Umständen hat auch die Benutzung eines Proxy-Servers, eingetragen unter

"Verbindungen - LAN-Einstellungen"

einen Einfluß auf das Sicherheitsverhalten und sollte im Problemfalle durch temporäres Abschalten überprüft werden. Die hier vorgenommenen Einstellungen können auch noch von den Filterfunktionen einer installierten Antivirensoftware wie NetShield/McAffee oder eines persönlichen Firewalls wie etwa @Guard überlagert werden.

**3.2.1 Internetoptionen "Sicherheit"**




Der Internet-Explorer unterscheidet zwischen den Sicherheitsbereichen "Internet", "Lokales Intranet", "Vertrauenswürdige" und "Eingeschränke Sites".

- Unter "Lokales Intranet" fallen alle URL-Adressen, die nicht voll qualifiziert, sondern nur mit dem Rechnernamen spezifiert werden. Die URL "zam123" oder auch "localhost" (IP-Adresse 127.0.0.1) liegen demnach im Intranet, während "zam123.zam.kfa-juelich.de" dem Internet zugerechnet wird.
- Vertrauenswürdige Sites sind solche, die eine sichere und zertifizierte "Secure Socket Layer"-Verbindung anbieten, die also durch Verschlüsselung des Datentransfers abhörsicher sind.
- Besonders risikoreiche Sites kann man von Hand unter "Eingeschränkte Sites" eintragen und dort die Sicherheitsanforderungen entsprechend höher setzen.

Die Unterscheidung zwischen Internet und Intranet ist meines Erachtens für große Netze mit Tausenden von Rechnern und sicherheitsmäßig "flacher" Struktur, zu denen auch JuNet zu zählen ist, nicht besonders relevant. Ein von Hackern übernommener Rechner im Intranet kann ein größeres Sicherheitsrisiko darstellen als ein gut geführter externer Server im Internet. Ähnliches gilt für eingeschränkte Sites, zu denen man am besten überhaupt keine Verbindung aufnimmt oder aber generell alle in der folgenden

Empfehlung erlaubten Dateninhalte auf "Eingabeaufforderung" konfiguriert, womit das Problem jedoch nur auf den aktuellen Zugriff vertagt ist. Der schwierigen Entscheidung, ob man den Zugriff erlauben will oder nicht, ist man damit nicht enthoben.

Aus diesen Gründen empfiehlt sich eine für Inter- und Intranet weitgehend oder tatsächlich identische Einstellung, die den praktischen Anforderungen einer ungehinderten Arbeit im Internet genügt, ohne den Benutzer dem besonders hohen Gefährdungspotential bestimmter Techniken (ActiveX, WSH, unsichere Scripting-Klassen etc.) auszusetzen. Die detaillierten Einstellmöglichkeiten zur Java-Sicherheit unter "Internetoptionen - Sicherheit - Stufe anpassen - Java Einstellungen - Benutzerdefiniert" werden ebenfalls nicht berücksichtigt, sondern auf den Default-Werten "Hohe Sicherheit" belassen.

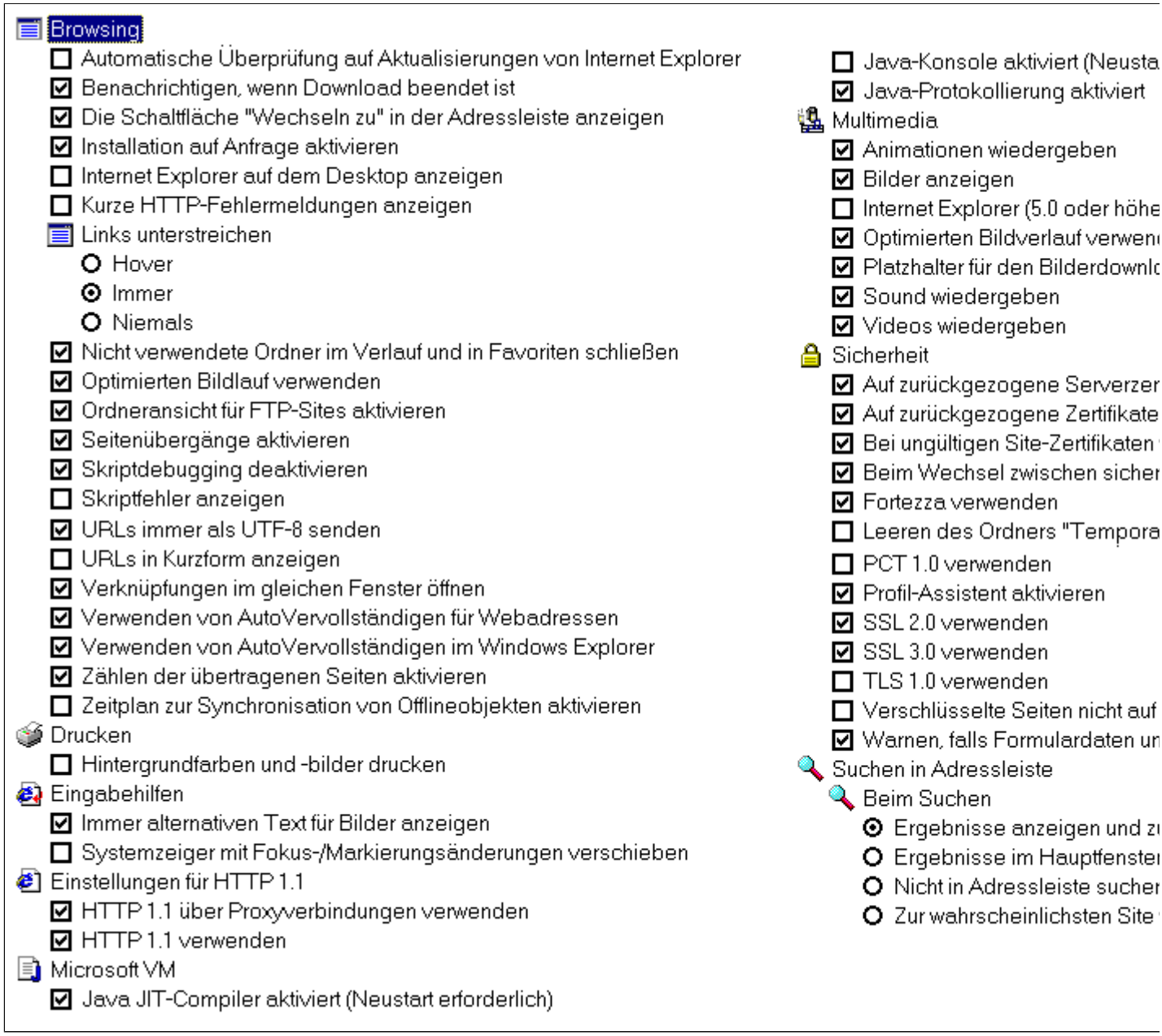
**Es muß jedoch deutlich darauf hingewiesen werden, daß mit den so empfohlenen Einstellungen keineswegs absolute Sicherheit beim Browsen im Internet gegeben ist!** Beispielsweise bedeutet bereits die Zulassung von "einfachem" Java/VBScript ein signifikantes Risiko. Da aber fast jeder Webserver heutzutage JavaScript benutzt, scheint ein Abschalten dieser Technik für ein ungehindertes Navigieren im Internet kaum praktikabel.


ActiveX-Steuerelemente und Plugins
ActiveX-Steuerelemente ausführen, die für Scripting sicher sind
Aktivieren
Deaktivieren
Eingabeaufforderung
ActiveX-Steuerelemente initialisieren und ausführen, die nicht siche
Aktivieren
Deaktivieren
Eingabeaufforderung
ActiveX-Steuerelemente und Plugins ausführen
Aktivieren
Deaktivieren
Eingabeaufforderung
Vom Administrator genehmigt
Download von signierten ActiveX-Steuerelementen
Aktivieren
Deaktivieren
Eingabeaufforderung
Download von unsignierten ActiveX-Steuerelementen
Aktivieren
Deaktivieren
Eingabeaufforderung
Benutzerauthentifizierung
Anmeldung
Anonyme Anmeldung
Automatische Anmeldung mit aktuellem Benutzernamen
Automatisches Anmelden nur in der Intranetzone
Nach Benutzername und Kennwort fragen
Cookies
Cookies annehmen, die gespeichert sind
Aktivieren
Deaktivieren
Eingabeaufforderung
Cookies pro Sitzung annehmen (nicht gespeichert)
Aktivieren
Deaktivieren
Eingabeaufforderung
Download
Dateidownload
Aktivieren
Deaktivieren
Schriftartdownload
Aktivieren
Deaktivieren
Eingabeaufforderung
Microsoft VM
Java-Einstellungen
Benutzerdefiniert
Hohe Sicherheit
Java deaktivieren
Mittlere Sicherheit
Niedrige Sicherheit
Scripting
Active Scripting
Aktivieren
Deaktivieren
Eingabeaufforderung
Einfügeoperationen über ein Skript z
Aktivieren
Deaktivieren
Eingabeaufforderung
Scripting von Java-Applets
Aktivieren
Deaktivieren
Eingabeaufforderung
Verschiedenes
Auf Datenquellen über Domänengre
Aktivieren
Deaktivieren
Eingabeaufforderung
Dauerhaftigkeit der Benutzerdaten
Aktivieren
Deaktivieren
Installation von Desktopobjekten
Aktivieren
Deaktivieren
Eingabeaufforderung
Programme und Dateien in einem IFI
Aktivieren
Deaktivieren
Eingabeaufforderung
Subframes zwischen verschiedenen
Aktivieren
Deaktivieren
Eingabeaufforderung
Unverschlüsselte Formulardaten übe
Aktivieren
Deaktivieren
Eingabeaufforderung
Ziehen und Ablegen oder Kopieren u
Aktivieren
Deaktivieren
Eingabeaufforderung
Zugriffsrechte für Softwarechannel
Hohe Sicherheit
Mittlere Sicherheit
Niedrige Sicherheit

Seite 1

### 3.2.2 Internetoptionen "Erweitert"

Einige wenige Einstellungen, die ebenfalls Auswirkung auf die Sicherheit des lokalen PCs haben können, finden sich noch im Menü "Erweitert". Das folgende Bild zeigt eine mögliche Auswahl der Einstellungen:




Seite 1

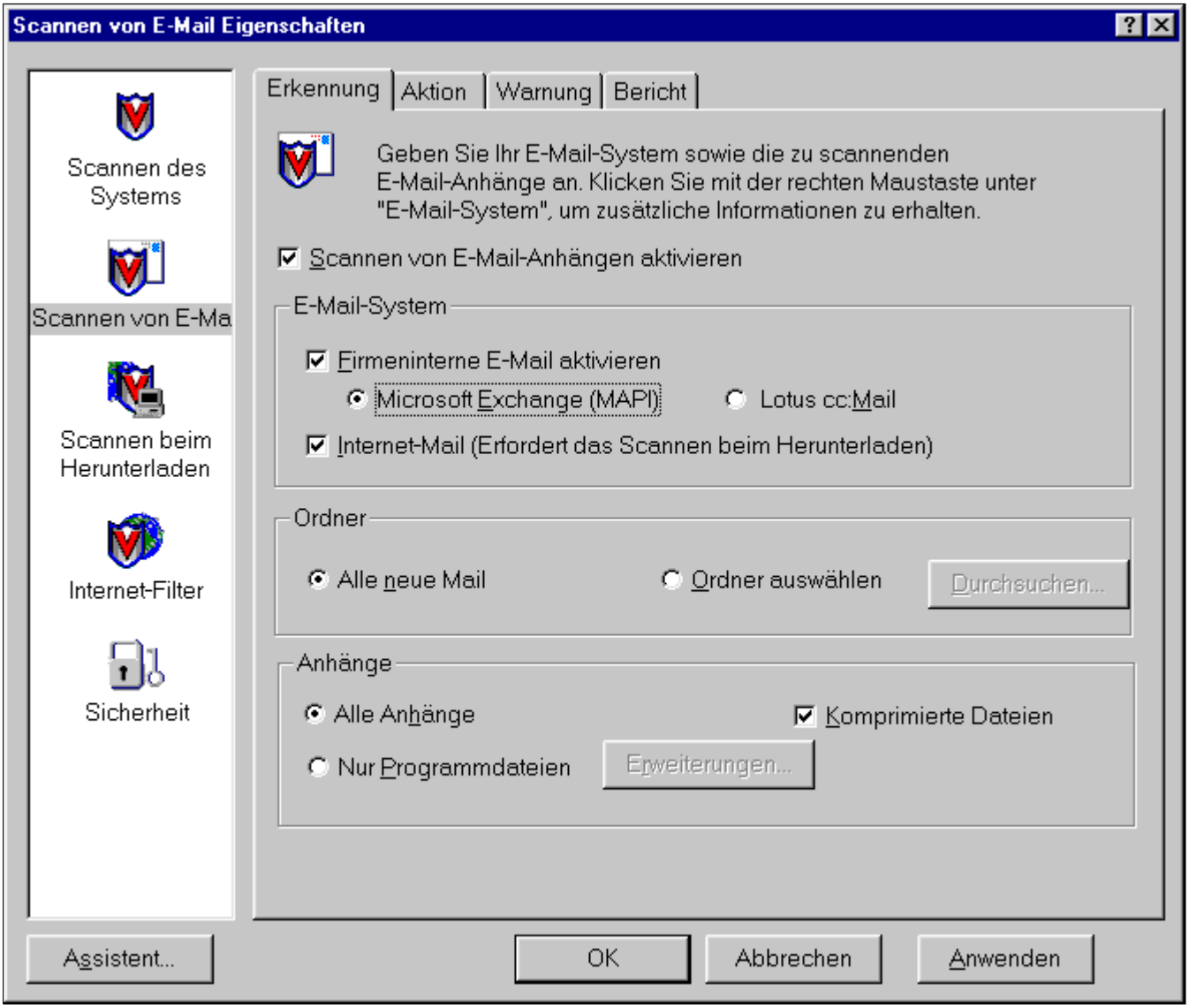
## 4. Antiviren-Programme

Es existieren inzwischen auf dem Markt eine Vielzahl an Antiviren-Programme, die alle ihre Stärken und Schwächen besitzen, so daß man zwangsläufig eine Auswahl treffen muß. Ein "gutes" Antivirenprogramm sollte aber jeder Rechner, der ans Internet angeschlossen ist, installiert und aktiviert haben ! Gut bewährt haben sich beispielsweise die im Forschungszentrum seit längerem angebotenen Antivirenprogramme

F-Prot und NAI Virusscan

für die das ZAM unter \\pcsrv.zam.kfa-juelich.de\public die Software und die aktuellen Virensignatur-Dateien zur Verfügung stellt.

Vorteil von NAI Virusscan ist neben der bewährten Aktualität und Vielzahl der angebotenen Virenfilter die gute Konfigurierbarkeit und die Möglichkeit, sowohl die Virensignaturen als auch die Software selbst regelmäßig automatisch oder auf Knopfdruck auf den neuesten Stand bringen zu können. Die Software unterstütz Virenalarme durch PopUp-Meldungen, durch Email und durch akustische Warnungen. Die Version "McAffee Virus Scan" enthält differenzierte Einstellmöglichkeiten für das Scannen des Systems, Scannen von Email undScannen beim Herunterladen von Dateien sowie eine einfache Firewall-Funktion, mit der aktive Inhalte (ActiveX und Java), IP-Adressen und Web-URLs gesperrt werden können:




Wer seine bereits installierte Antivirensoftware kurz testen möchte, kann versuchen, die Datei "**EICAR.DAT**" herunterzuladen. Sie enthält eine standardisierte Virensignatur ohne Funktion, die zum Testen von Antivirensoftware benutzt wird und von jedem Virenscanner erkannt werden sollte (es handelt sich ***nicht*** um ein echtes Virus!).

Weitere Informationen zur Sicherheit und zu neuen Entwicklungen stellt das ZAM auch unter

http://www.fz-juelich.de/zam/net/security

zur Verfügung.

Seite 1

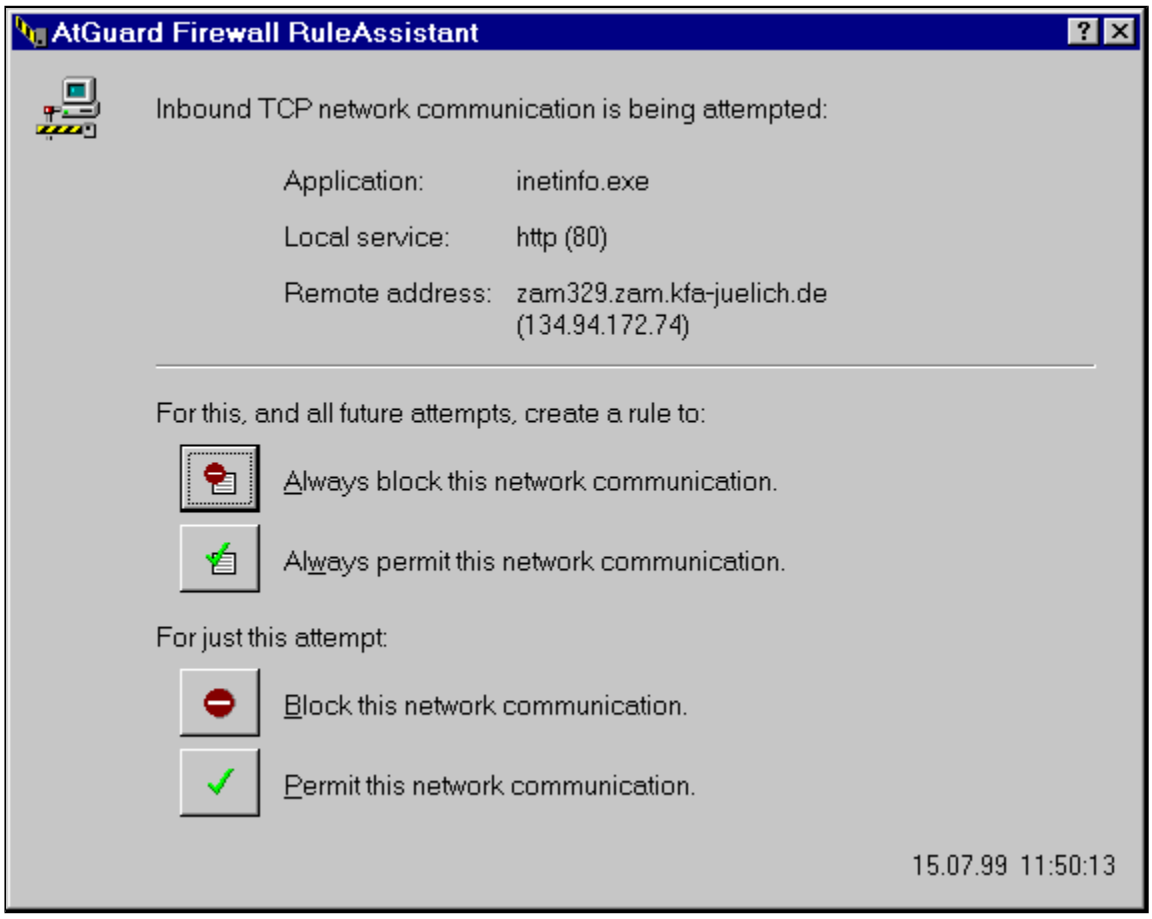
## 5. @Guard: Ein Firewall für Internet-PCs

AtGuard ist ein Webfilter und persönlicher Firewall zur Überwachung und Steuerung der Zugriffe aus dem Netz auf einen ans Internet angeschlossenen Windows-PC. Neben regelbasierten Filtermöglichkeiten auf der Basis von Internet-Adressen und -Applikationen (IP-Port und Anwendung) bietet AtGuard zusätzliche Filtermöglichkeiten für das Browsen im World Wide Web wie etwa Werbe-, Cookie- oder Mail-Address-Filter. Auch die Möglichkeit, domänenspezifisch die Ausführung aktiver Inhalte wie Scripting, Java, ActiveX und Popup-Fenster zu unterbinden, ist sicherheitstechnisch interessant.

AtGuard unterstützt selbslernend den Aufbau eines nach den Bedürfnissen des Benutzers "maßgeschneiderten" Firewalls durch eine dialoggeführte Regelerstellung, die automatisch beim Versuch eines Verbindungsaufbaus aus dem Netz aktiviert werden kann. Solche Regeln können für die gerade aktive Anwendung, für bestimmte Kommunikationspartner und Ports oder generell systemweit definiert werden.

Neben einem "Dashboard", das die Netzwerk- und Filteraktivitäten von AtGuard im Stile einer Taskleiste "gedocked" oder als normales Fenster anzeigt, werden konfigurierbare Ereignis-Logs und anwendungsspezifische IP-Statistiken der Netzzugriffe erstellt.

Besonders wichtig ist die Funktion des Regelassistenten als Monitor für unerwartete oder unerwünschte Zugriffsversuche ("Hacker Scans") aus dem Netz: Für jeden Verbindungsversuch, der nicht durch eine der vordefinierten Firewallregeln erfaßt ist, erscheint ein PopUp-Fenster mit zusätzlichen Informationen wie Uhrzeit, IP-Adressen des Verbindungsaufbaus und beteiligte IP-Ports (Dienste). Das folgende Beispiel zeigt ein solches Fenster für einen Verbindungsversuch des Rechner zam329 zu einem auf dem PC laufenden Webserver (Port 80):




Eine detaillierte Beschreibung der Funktionen von AtGuard und ausführliche Konfigurationshinweise für den Betrieb im JuNet sind im ZAM-internen Bericht

http://www.fz-juelich.de/zam/docs/printable/ib/ib-99/ib-9916.pdf

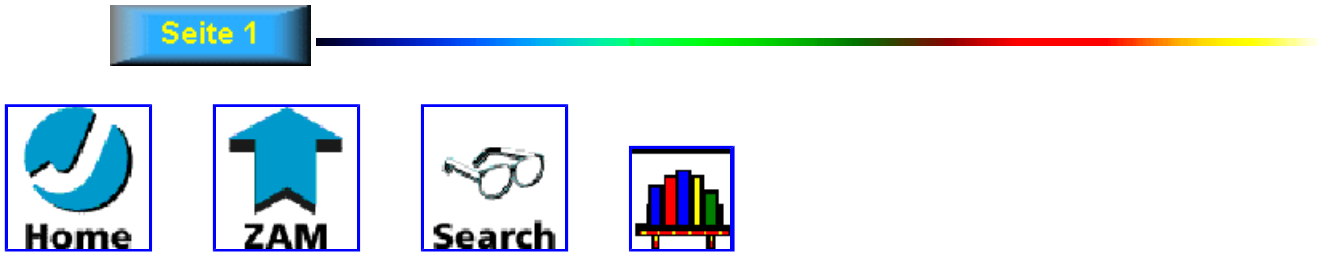
und in der technischen Kurzinformation ZAM-TKI-0439 unter

http://www.fz-juelich.de/zam/docs/tki/tki_html/t0349/t0349.html

zu finden. Die Software wird paßwortgeschützt für den Download durch die PC-Verantwortlichen der Institute unter

**\\zelcds.zel.kfa-juelich.de\atguard**

angeboten.




---

*J.Meißburger , Forschungszentrum Jülich, FZJ-ZAM, dokumentation.zam@fz-juelich.de*