

Vortrag über Sicherheit im Internet vom 08.04.2003
Brem Thomas

Man hört in letzter Zeit oft in den Medien von gefährlichen Mails die die Existenz ganzer Firmen oder Verwaltungen bedrohen oder plötzlich gelöschte oder geänderte Internetseiten oder mögliche Zugriffe ohne Passwörter auf Firmen-Intranets die nicht für die Öffentlichkeit gedacht sind.

So ist es Ende letzten Jahres Microsoft selbst passiert dass der deutsche Server offen stand und man Firmeninterne Dokumente und Quelltexte downloaden konnte.

Wie kann man sich nun dagegen schützen ?

Es gibt kein Wundermittel um seinen eigenen PC absolut sicher zu machen, man muss Kompromisse mit seinen gewünschten Anwendungen die laufen sollten (Bank, Mail, Webformulare) und den offenen Scheunentoren die Windows oftmals bietet eingehen.

Und auch die Kombination der verschiedenen Betriebssysteme 95, 98, ME, NT, 2000, XP und der Browser IE, Netscape, Opera bieten immer wieder Überraschungen, da sich oftmals ein Browser auf einem System anders verhält wie auf einem anderen.

Wichtig ist, immer aktuelle Servicepacks, Sicherheitsupdates und Patches einzuspielen.

Seit Windows 98 SE verfügen MS-Windows Betriebssysteme über Funktionen zum Update über das Internet. Die Funktion findet sich im allgemeinen direkt im Startmenü. Sofern sie dort nicht (mehr) vorhanden ist, sucht man nach der Datei wupdmgr.exe.

Das Programm startet den Internet-Explorer mit der Seite <http://windowsupdate.microsoft.com>. Für die Durchführung des Updates ist es erforderlich, daß die Ausführung von ActiveX-Elementen zugelassen wird. Wenn Sie den Punkt 'Produktupdates' anklicken, wird die aktuelle Systemkonfiguration ermittelt und verfügbare Updates werden angezeigt. Sie können dann auswählen, ob und welche Updates heruntergeladen und installiert werden sollen.

Seit Windows ME steht außerdem die Möglichkeit automatischer Updates zur Verfügung. Sie finden die Funktion unter START/Einstellungen/Systemsteuerung. Sofern die Funktion aktiviert ist, wird bei einer bestehenden Internetverbindung nach neuen Updates gesucht. Je nach Einstellung erfolgt eine Benachrichtigung über vorhandene Updates oder sie werden automatisch im Hintergrund heruntergeladen. Der Anwender kann dann entscheiden, welche Updates installiert werden sollen. Ich bin eigentlich gegen die automatischen Updates, da dann alles was MS irgendwie loswerden will ohne es zu wissen plötzlich auf dem Rechner ist. Z.b. der IE mit sämtlichen Sprachen, oder Treiberupdates die meistens schief gehen wie ich die Erfahrung gemacht habe.

Man kann auf dieser Seite per Hand die Updates mit Erklärung genau auswählen und nur die wichtigen installieren.

Wenn man jetzt sein System auf einem aktuellen Stand hat
Kann man einige Hilfreiche Software installieren.

Da wäre ein guter Virens scanner ein guter Anfang,
z.b. von McAfee, Norton, Sophos wie ihr sie alle kennt.

Es gibt verschiedene Virenarten

Viren: Ein Computer-Virus ist ein in böswilliger Absicht geschriebener Programm-Code, der sich in Programme oder Dateien einfügt und dort Fehlfunktionen und Störungen verursacht. Wie ein biologischer Virus kann sich auch der Computer-Virus vermehren, indem er andere Datenträger "infiziert". Viren können durch aus dem Internet heruntergeladene Dateien, mit E-Mail oder über Disketten übertragen und verbreitet werden. Oft wissen die Überträger des Computer-Virus nicht, dass sie infizierte Programme oder Disketten weiterreichen. Der Virus bleibt solange inaktiv, bis bestimmte Umstände die Ausführung seines Codes durch den Computer auslösen. Manche Viren sind reine Spielerei, die nichts anderes tun, als den Benutzer durch sinnlose Aktionen an der Arbeit zu hindern und haben nur harmlose Auswirkungen. Andere können sehr schädlich sein, indem sie Daten löschen oder die Neuformatierung von Festplatten veranlassen. Zurzeit sind mehr als 20000 Computerviren bekannt.

Im Allgemeinen unterscheidet man drei Hauptklassen von Viren:

- **Dateiviren** hängen sich an Programmdateien, meist ausgewählte .COM- oder .EXE-Dateien. Einige können jedes Programm infizieren, dessen Ausführung angefordert wird, einschließlich Dateien mit den Endungen .SYS, .OVL, .PRG und .MNU. Sobald ein solches Programm geladen wird, wird der Virus aktiv.
- **System- oder Boot-Sektorviren** infizieren den ausführbaren Code, der sich an bestimmten Stellen von Festplatten oder Disketten befindet. Sie nisten sich in den Boot-Sektor auf Disketten oder den Master-Boot-Record auf Festplatten ein.
- **Makroviren** sind Viren, die Datendateien infizieren. Sie werden typischerweise in Microsoft Office Dokumenten (.doc, .dot, .xls) gefunden. Sobald ein infiziertes Dokument geöffnet wird, wird die Datei Normal.dot infiziert. Wird

anschließend ein Dokument gespeichert/geöffnet, wird dieses mit dem Virus infiziert. Makroviren können beispielsweise den Speichern-Befehl durch den Format-Befehl ersetzen.

Immer öfter werden Viren in der Anlage einer E-Mail verschickt. Eine solche Mail zu öffnen ist noch nicht schädlich. Das Verhängnisvolle ist jedoch, dass die meisten E-Mail-Clientprogramme bei Doppelklick auf die Anlage versuchen, diese mit dem Originalprogramm zu öffnen. Handelt es sich bei der Anlage um eine Script-Datei, wird diese ausgeführt.

Würmer: Würmer sind ein Sonderfall von Viren, die sich selbst von infizierten Rechnern aus per E-Mail weiterverbreiten. Als Beispiel sei hier der im Mai 2000 aufgetauchte "ILOVEYOU"-Wurm, dessen Wirkungsweise grossen Schaden anrichtete, erwähnt.

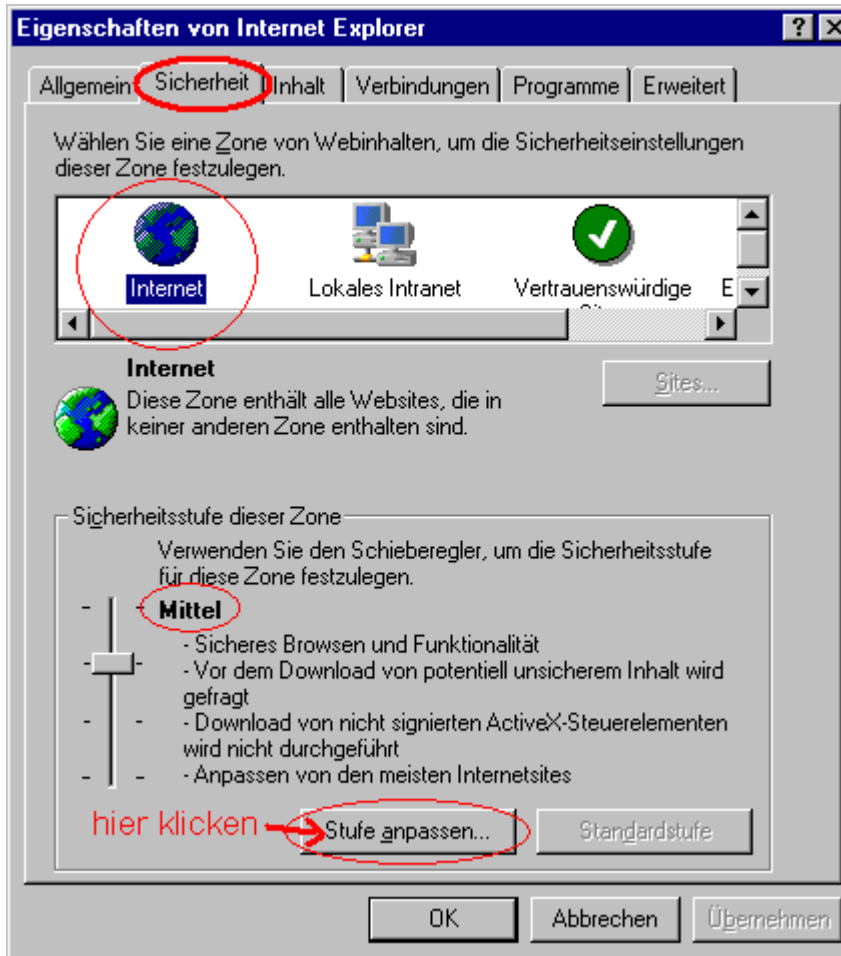
- **Trojanische Pferde, Trojaner:** Werden mit einer anderen Anwendung unbemerkt installiert, um den Rechner auszuspionieren, und Zugriff von außen zu ermöglichen.
- **Adware:** Ähnlich wie Trojaner, werden mit einem anderen Programm installiert und sammeln Daten über den Benutzer, die sie über das Internet an eine bestimmte Adresse verschicken.
- **Spyware:** Ein Spezialfall. Diese Programme werden in der Regel von Personen installiert, die direkten Zugang zum System haben. Sie dienen dazu, gezielt Informationen über den Benutzer zu sammeln und z.B. Passwörter und Inhalte von E-mails auszuspionieren. Sie werden auch eingesetzt, um das Surfverhalten und die Arbeitsgewohnheiten des Benutzers zu protokollieren.

Die modereren Virens Scanner können eigentlich alle dieser Typen Erkennen und soweit möglich reparieren. Ich kann hier einen kostenlosen Virens Scanner namens Antivir empfehlen, er ist nur ca. 3,5 MB groß und arbeitet recht stabil, auch auf älteren Systemen (mit Onlineupdatefunktion) der auch Standard bei allen Virens Scannern ist.

Als nächstes sollte man gleich noch einen 0190-Warnen (YAW) installieren oder besser die kostenpflichtigen Nummern bei der Telekom Direkt sperren lassen (kostet einmalig ca 15 Euro)

Dann kommen wir zum Browser selbst, wo man sehr viel Einstellen kann. Ich nehme hier den IE, mit den anderen gibt es die gleichen Oder ähnlichen Optionen.

In die Einstellungen des Browsers kommt man mit dem Rechts-Klick auf den IE und Einstellungen.



In der Registerkarte "Sicherheit" sollten mehrere Änderungen vorgenommen werden:

Leider sind die Standard-Einstellungen des MS Internet Explorer (in allen Versionen) selbst in der Stufe "Höchste Sicherheit" immer noch "Scheunentore" für Viren, Trojaner und Co.

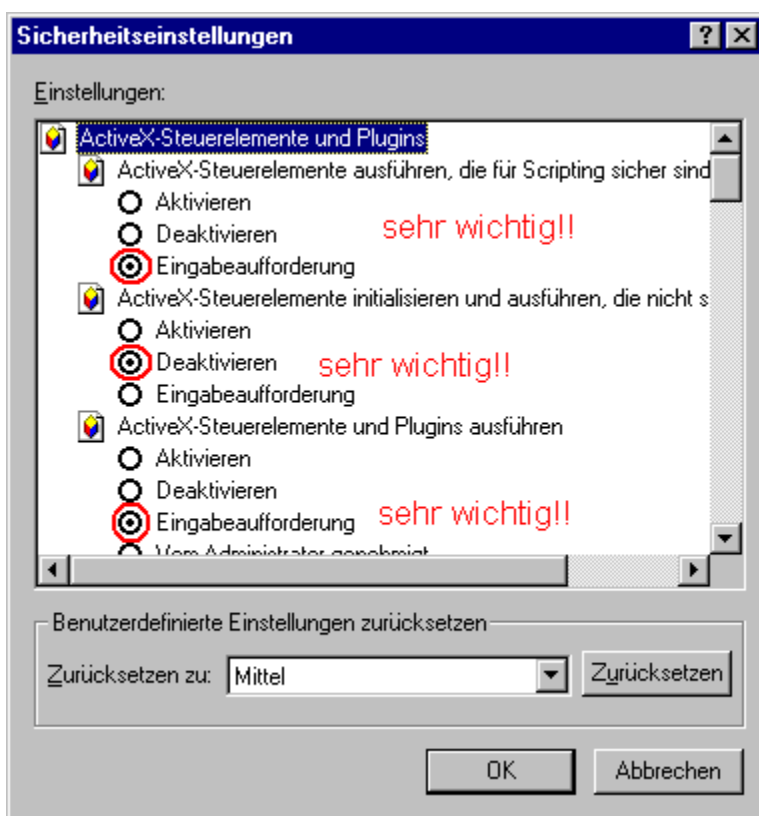
Um die vorgeschlagenen Einstellungen verstehen zu können, seien ein paar Worte zum gesamten Sicherheitskonzept im

MSIE gesagt. Der MSIE teilt das gesamte Internet - also alle Dienste, die über den Browser erreichbar sind - in vier Zonen auf:

- Internet: enthält alle Websites, die in keiner anderen Zone enthalten sind.
- Lokales Intranet: enthält alle Websites im Intranet, in dem der MSIE läuft, also im lokalen Netzwerk und im Netzwerk des verwendeten Proxyserver.
- Vertrauenswürdige Sites: Liste von individuellen Sites, denen Sie vertrauen.
- Eingeschränkte Sites: Sites, denen Sie eher nicht vertrauen.

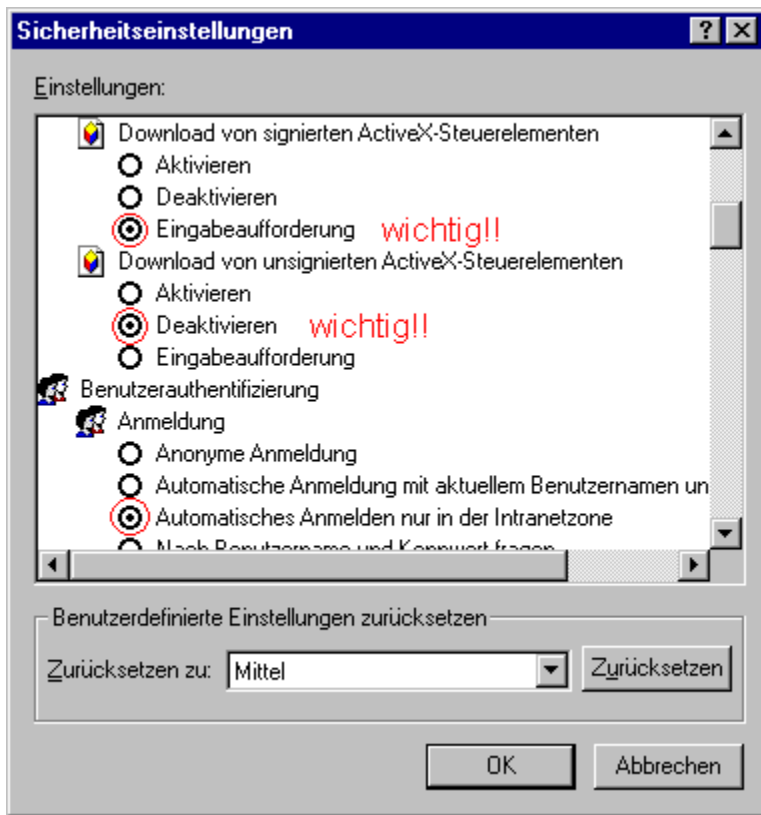
Jede einzelne dieser Zonen kann individuell konfiguriert werden. Für jede Zone kann man außerdem eine von vier möglichen Sicherheitsstufen auswählen: hoch, mittel, niedrig, sehr niedrig. Diese

vier Sicherheitsstufen wiederum sind bereits vorkonfiguriert, es empfiehlt sich jedoch unbedingt eine genauere Kontrolle, weil man nicht unbedingt einverstanden sein muss mit den Voreinstellungen.



- **Besonders die sog. ActiveX-Steuererelemente stellen eine grosse Gefahr bezüglich unerwünschte Zugriffe aus dem Internet auf den lokalen PC dar! ActiveX-Controls (AXC) sind kleine Windows-Programme. Diese werden automatisch von einer Webseite auf Ihren Rechner geladen und dort ausgeführt. Ist ein solches AXC bereits auf Ihrem Computer gespeichert, wird es beim Aufruf der Seite gestartet. Zum Sicherheitsrisiko**

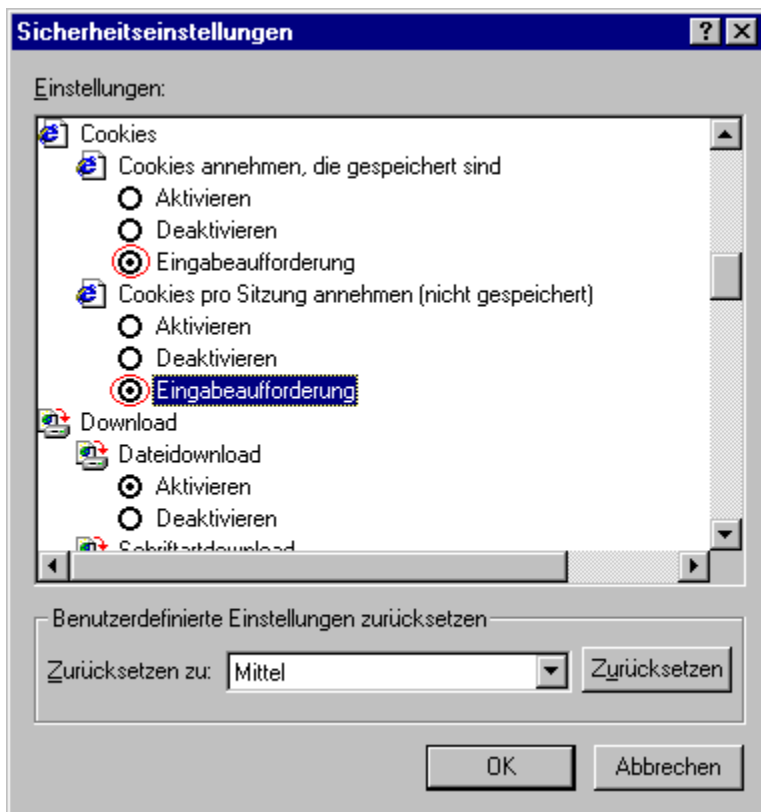
werden diese
Controls, weil sie
sehr eng mit dem
Betriebssystem
verflochten sind. Auf
deutsch: mit einem
ActiveX-Control lässt
sich alles machen,
was auch mit
Tastatur und Maus
machbar ist. Ein
böartiger
Webmaster könnte
beispielsweise ein
Control
programmieren,
dass Ihrem Rechner
befiehlt, sämtliche
Daten auf der
Festplatte zu
löschen. Betreten
Sie seine Seite, tritt
das AXC in Aktion -
mit entsprechenden
Folgen. So werden
beispielsweise viele
Webdialer über
ActiveX automatisch
heruntergeladen und
gestartet.



Auch hier sind die Einstellungen bezüglich ActiveX sehr wichtig!!

Die Angabe zur Benutzerauthentifizierung

Sollte nur in der Intranet-Zone aktiv sein.



zum Abschnitt "Cookies"

durch Klick in den kleinen Kreis die Option "Eingabeaufforderung" aktivieren!

Das Prinzip der Cookies setzt auf kleine Textdateien, die beim Besuch vieler WebSites als "Datenmüll" auf der lokalen Festplatte verbleiben und mit der Zeit vergessen

werden. Cookies werden hauptsächlich eingesetzt, um Besuchern von WebSites personalisierte Informationen anbieten zu können. Zu diesem Zweck wird der Cookie-Datei eine ID beigefügt, manchmal auch einen Hinweis auf die benutzte IP-Adresse, Hinweise auf bereits besuchte andere Sites und vieles mehr.

Dies ist die positiv ausgedrückte Eigenschaft eines Cookies.

Die negative ist, das Cookies durchaus auch zur Datenspionage taugen, die bis in die Spionage von Passwörtern oder anderen brisanten Bereichen reichen. Denn eigentlich war es vorgesehen, den Zugriff auf Cookies der Site zu erlauben, von der die Datei auch lokal gespeichert wurde. Ein Fehler im Internet-Explorer erlaubt jedoch auch einen erweiterten Zugriff auf Cookies. Das heißt, fügt eine Website mit böser Absicht hinter ihre URL für die

weitere Navigation statt einem Slash ein Prozentzeichen ein, Beispiel:

`http://www.url.de%xxx%2xxx%2xxx%3F.yyy.com,`
überspringt der Microsoft-Browser die Prozentzeichen und behandelt die zuletzt genannte Adresse, in unserem Fall `yyy.com` so, als befände man sich auf der Seite. Damit lassen sich auf der feindlichen Webseite die gespeicherten Cookies Informationen anzeigen.

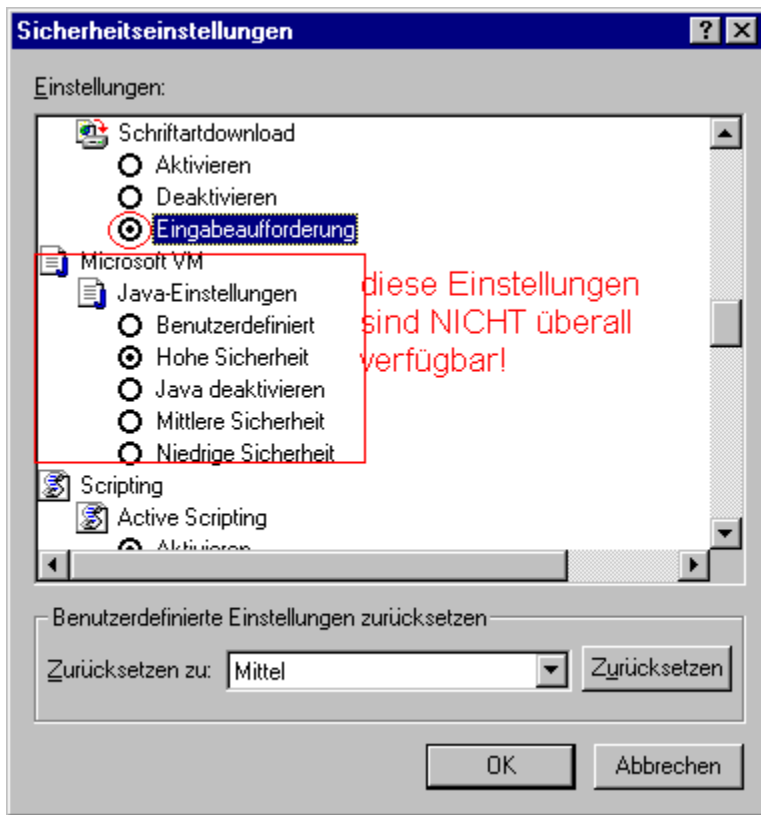
Der Internet Explorer öffnet somit über die Cookie-Verwaltung einer feindlich gesinnten und präparierten Webseite den Zugang zu den Cookies des jeweiligen Besuchers. Je nach Art der Cookies tauchen damit auch sensible Informationen im Klartext auf. Netscape Browser sind übrigens von diesem Problem nicht betroffen.

Verlässt man sich auf die automatische Leerung der temporären Internet-Dateien

und der Offline-Inhalte (diese Option kann unter Einstellungen des Internet-Explorers eingestellt oder manuell ausgelöst werden), verbleiben Cookies unangetastet in diesem Verzeichnis und können während der nächsten Online-Sitzung ausgelesen werden.

Man sollte von Zeit zu Zeit im Cookie-Verzeichnis die nicht benötigten löschen.

Aufgrund der Brisanz wird Microsoft in zukünftigen Versionen des Internet-Explorers eine erweiterte Cookie-Verwaltung implementieren die unter anderem darauf hinweisen wird, ob Cookies auch von Drittseiten abgerufen und gespeichert werden dürfen.!



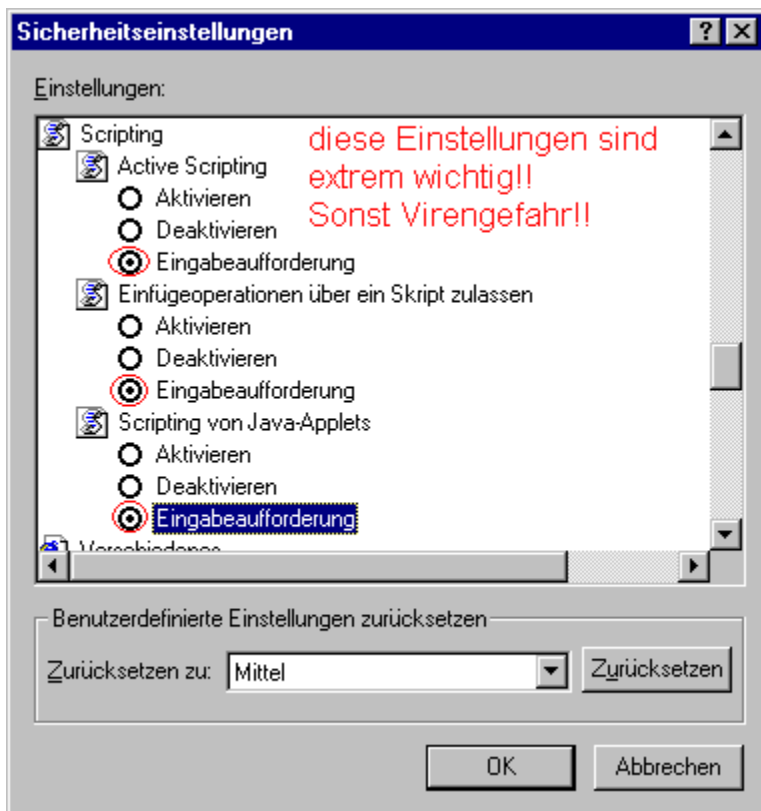
Der Schriftartendownload ist prinzipiell unerwünscht!!

Nur im begründeten Einzelfall (nachfragen / Bescheid geben!!) wird er geduldet!! Deshalb: *"Eingabeaufforderung"*

Die Microsoft VM (Virtual Machine, um Java ausführen zu können) ist nicht überall installiert, deshalb sind diese Optionen auch nicht auf jedem PC aufgeführt.

Benutzerdef. Zeigen.

Die Rubrik *"Scripting"* ist wieder sehr sensibel bezüglich Viren, Trojanern und Co.!!



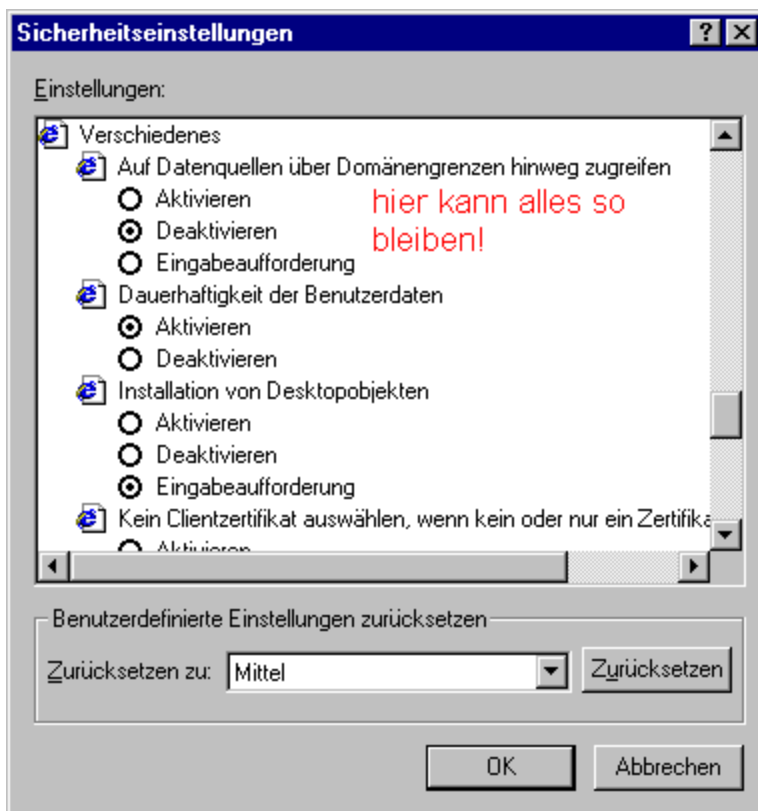
Solche Scripts werden leider (wie auch Cookies) immer häufiger in vielen Websites eingesetzt, sodass das surfen unter diesen Einstellungen manchmal zur Qual werden kann, da man ständig die Annahme von Cookies oder die Ausführung von Scripten per Mausklick bestätigen oder verweigern muss. Da

aber über 80% der gefährlichen Viren etc. gerade die Unzulänglichkeiten des MS Internetexplorers ausnutzen, sind diese Einstellungen extrem wichtig und man muss von Website zu Website versuchen, zu entscheiden, ob man sich auf "gefährlichem oder harmlosen Territorium" bewegt.

Im Zweifelsfall Cookies und Scripte ablehnen!!#

- - **Java** ist eine von der Firma "Sun" entwickelte Programmiersprache . Auch Java läuft direkt auf Ihrem Rechner, ermöglicht Außenstehenden in der Regel aber keinen Zugriff auf Ihre Daten, da es in einer abgeschlossenen Umgebung ("Sandbox") abläuft. **Nur bei** Programmierfehlern

ist der Zugriff auf Ihre Daten möglich. Da solche Fehler in der Vergangenheit **aber öfter** vorgekommen sind, wird auch hier zur erhöhten Vorsicht geraten.



Alle nachfolgenden Einstellungen können wie voreingestellt bleiben.

(Die nebenstehenden Bilder sind nur der Vollständigkeit halber aufgeführt)

- "Auf zurückgezogene Zertifikate überprüfen" einschalten
- PCT 1.0 ausschalten, wird nicht benötigt und enthält evtl. unnötige Sicherheitslücken.
- "Verschlüsselte Daten nicht auf der Festplatte abspeichern" einschalten
- "Gespeicherte Seiten beim Beenden des Browsers löschen" einschalten

Damit wäre der Browser einigermaßen sicher konfiguriert.

Jetzt noch kurz etwas zum DFÜ-Netzwerk,

man sollte sich unbedingt die Protokolle anschauen woran die

DFÜ-Verbindung gebunden ist, es ist nur TCPIP nötig,

wenn NETBIOS oder Datei u. Druckerfreigabe installiert ist

kann man mit einfachen NET-Befehlen (share, use) auf den

Rechner zugreifen wenn man die IP-Adresse weiss die derjenige

beim Verbindungsaufbau erhalten hat.

Dann gibt es bei XP und Windows 2000 noch den Nachrichtendienst

Den man unbedingt abschalten sollte,

jede der ein solches System hat und eine Wählverbindung aufbaut

(gilt nicht für Router und Proxyserver) kriegt oft plötzlich eine

Meldung eingeblendet die man mit OK bestätigen muss.

Abschalten zeigen.

Firewalls - Nützlich, aber kein Patentrezept

Das Funktionsprinzip der Firewall

Übersetzt man das englische Wort Firewall ins Deutsche, so versteht man darunter eigentlich eine Brandschutzwand, also eine spezielle Mauer, die das Übergreifen der Flammen von einem Gebäudeteil auf ein Anderes verhindert. In der Computerwelt ist eine Firewall eine Software- oder Hardwarelösung, die zwischen zwei Netzwerke geschaltet wird, und den Datenverkehr zwischen diesen beiden Netzwerken filtert. Man könnte sich eine Firewall wie einen Pförtner vorstellen, der alle ankommenden und ausgehenden Daten einer Art Gesichtskontrolle unterzieht und anhand dessen entscheidet, wen er durchlässt und wen eben nicht.

Wer sich im Internet bewegt, ist grundsätzlich der Gefahr von Angriffen ausgesetzt. Dies können echte und bösartige **Attacken auf den Rechner** sein, zumindest aber Zugriffsversuche auf persönliche und private Daten. Hacker werden zwar nur selten **Angriffe auf Hobbysurfer** unternehmen. Ausgeschlossen ist freilich auch dieses nicht, ebenso wenig die Versuche so genannter Script-Kiddies, aus falsch verstandenem Ehrgeiz oder schlichter Boshaftigkeit fremde Computer zum Absturz zu bringen. Weitaus größer allerdings ist die Gefahr einzuschätzen, zum Opfer krimineller Angreifer zu werden, die durch das Ausspähen sensibler Daten wie Kreditkartennummern oder Passworten echten finanziellen Schaden anrichten können.

Wenn wir beim Bild des Pförtners bleiben, lässt sich auch die Problematik einer Firewall gut darstellen: Damit der Pförtner seine Aufgabe erfüllen kann, muss man ihm zuvor genau erklären, anhand welcher Kriterien er entscheiden soll, wen er durchlassen darf, und wen nicht. Zurück in der Computerwelt stellt gerade diese Definition der “Durchlass-Kriterien”, in der Fachsprache “Ruleset” oder Regelsatz genannt, für den Laien häufig ein Problem dar. Zudem muss sichergestellt sein, dass tatsächlich alle Daten über die Firewall geleitet und dort gefiltert werden. Gibt es auch nur einen “Hintereingang”, ist die Firewall so gut wie nutzlos. Und noch ein dritter Punkt muss sichergestellt sein: Es genügt nicht, dass der “Pförtner” nur die am PC ankommenden Daten überwacht. Er muss auch die Programme überwachen, die vom PC aus ins Internet hinaus wollen. Gelingt es nämlich einem Angreifer, ein entsprechendes Programm (etwa ein Trojanisches Pferd oder Spyware) auf dem Rechner zu platzieren, könnten private Daten sonst ungehindert ihren Weg ins Netz finden.

Die häufig geäußerte Feststellung von Computerexperten, dass Firewalls für private Nutzer eigentlich nutzlos seien, hat aufgrund der oben dargestellten Problematik sicherlich seine Berechtigung. Und trotzdem machen Firewalls auch im privaten Bereich Sinn. Sie mögen ernsthaft durchgeführte Angriffe auf den Rechner nicht in allen Fällen abwehren. Aber wer tatsächlich die kriminelle Energie aufbringt, eine kleine Firewall zu “knacken”, würde vermutlich auch vor einer großen und ausgereiften Brandschutzwand nicht Halt machen. Gerade, weil Personal Firewalls für den privaten Gebrauch inzwischen vielfach günstig oder sogar kostenlos zu bekommen sind, sollte man nicht auf sie verzichten.

Wichtig: Allein die Tatsache, dass Sie auf Ihrem Rechner eine Firewall laufen haben, wird Sie niemals vor echten Angriffen - gleich welcher Art - schützen können. Denn

eine Firewall ist immer nur so gut wie ihr Benutzer. Wer sich also tatsächlich mit einer Firewall absichern will, sollte zumindest die Grundbegriffe des Datenverkehrs im Internet kennen.

Lösungen

Für private Nutzer, die gewöhnlich keine allzu sensiblen Daten auf ihrem Rechner haben, genügt in der Regel der Einsatz einer so genannten Personal Firewall. Darunter versteht man ein Programm, das anhand bestimmter Regeln entscheidet, welcher Datenverkehr zwischen PC und Internet erlaubt wird, und welcher nicht (ein so genannter Paketfilter). Dem Benutzer bleibt es, diese Regeln festzulegen. Gerade bei Personalfirewalls ist dies nicht allzu schwierig, da die Entwickler bereits einige wichtige Grundregeln vorgeben.

Hilfreich ist in allen Fällen der so genannte Lernmodus: Jedes Mal, wenn eine neue Verbindung ankommt oder abgeht, muss der Benutzer entscheiden, ob er dies künftig zulassen will oder nicht. Das Programm "merkt" sich diese Entscheidung dann für die Zukunft.

Zu den bekanntesten, wenn auch nicht besten, Personal Firewalls zählt Zonealarm von Zonelabs. "ZA" ist in einer kostenlosen Version erhältlich, genügt den Ansprüchen privater Nutzer und ist zudem auch für Laien einfach zu handhaben.

Ähnlich empfehlenswert sind etwa

- Sygate Personal Firewall (SPF)
- Norton Personal Firewall
- Tiny Personal Firewall

Wenn man sich ins Internet einwählt und eine Webseite aufrufen möchte, versucht der Browser eine Verbindung über das Protokoll TCP/IP auf den Port 80 aufzubauen. Damit wird der Dienst als http identifiziert.

Ein Server erwartet also am "anderen Ende der Leitung" (Port 80) auf eingehende Verbindungen. Dabei befindet er sich im sogenannten Listen - Modus. (er " lauscht")

Wenn dieser Server nun die Verbindung erkannt hat, antwortet er mit einer Bestätigung. Nun kann der Datenaustausch stattfinden.

Wenn man sich mit Sicherheitslöchern im Internet beschäftigt, sind das allerwichtigste die Ports.

Ein Port ist eine Schnittstelle zu einem Dienst und besitzt bestimmte Werte. Ports bis zum Wert 1024 sind für Server und Systemdienste reserviert.

Der Zugriff auf einen Port erfolgt also meist über diesen Wert hinaus.

Die Firewall beobachtet den "Verkehr" durch diese Ports ganz genau, und meldet bestimmte Bewegungen.

Dabei lassen sich bei komplexeren Firewalls Regeln aufstellen, um bestimmte Protokolle oder Ports einfach sperren zu lassen.

Bei den Personal-Firewalls muss man sich meist auf die Entscheidung des Programms verlassen.

Nur ein offener Port in einem System kann wiederum Verbindungen zu anderen Systemen aufnehmen. Darum sind "offene Ports" bei Hackern so beliebt. Man muss diese Eingänge unbedingt verschließen. Es gibt sogenannte Portscanner mit denen man den eigenen oder fremde PC auf offene Ports untersuchen kann.
(z.B. TCP View)

Für "Otto Normalverbraucher" am heimischen PC kommt also nur die Personal Firewall in Betracht. Heute werden Firewalls als Softwarepakete verkauft. Die Firewall installiert sich direkt in das TCP/IP - Protokoll, wo die entsprechend konfigurierten Filter eingesetzt werden.

|

[Zonealarm](#) ist als kostenlose Testversion erhältlich, und leicht zu installieren. Ein Assistent leitet ziemlich gut durch die Installation.

Die Firewall kontrolliert im aktiven Zustand alle Datenverbindungen zwischen dem Computer und dem Internet.

Neueinsteiger erschrecken sich häufig, wenn sich die Firewall das erste Mal meldet. Also keine Panik. Man muss bedenken, dass sich das Programm zunächst an die Umgebung gewöhnen muss.

Erkennt die Firewall z.B. eine unbekannte Anwendung, gibt sie einen entsprechenden Hinweis.

Grundsätzlich hat man nur 3 Möglichkeiten

- 1) Yes = Zugriff erlauben (wenn bedenkenlos)
- 2) No Zugriff verweigern (nicht bedenkenlose Anwendung)
- 3) Anwendung wird je nach Einstellung in Zukunft immer zugelassen, oder verweigert.

Im interaktiven Modus (Programms) von ZoneAlarm kann man die Zugriffsregeln verändern.

Der Aufbau gleicht dem Explorerfenster.

Mit rechter Maustaste auf einen Eintrag klicken

Im Kontextmenü kannst du nun die Regeln einstellen

Allow = zulässig

Dissallow = unzulässig

Ask= immer interaktive Rückfrage des Programms

Remove=Anwendung aus der Datenbank entfernen

Wenn jemand lieber eine Firewall in deutsch haben

möchte wäre Nortons Firewall empfehlenswert, die mit deutscher Beschreibung und pflegeleichter Installation im Handel für ca.60 Euro erhältlich ist.

Integrierter Firewall

Pro: Windows XP bietet dem Anwender eine eigene Firewall-Funktion. Damit kann der Benutzer seinen Rechner vor Angriffen aus dem Internet schützen. Eine DFÜ-Netzwerkverbindung ins Internet lässt sich zumindest bei Einzelplatzrechnern einigermaßen sichern.

Die Konfigurationsmöglichkeiten bieten lediglich die Freigabe der Standard-Internet-Ports an, etwa Port 80 für HTTP. Alle anderen Anschlüsse bleiben zunächst blockiert. Um zusätzliche Anschlüsse zu konfigurieren, etwa für ICQ, braucht man tiefer gehende Netzwerkkennntnisse. Das Programm lässt sich nicht so einrichten, dass das lokale Netzwerk von der Firewall-Funktion ausgeschlossen wird.

Wendet man also den Firewall mit den Standardeinstellungen auf eine lokale Netzwerkverbindung an, wird diese weitgehend eingeschränkt. Der Anwender kann danach nicht mehr auf die Freigaben des abgeschotteten Rechners zugreifen. Zudem wird er nicht gewarnt, wenn ein Rechner von außerhalb eine Verbindung zu seinem Rechner herzustellen versucht.

Ein Trojaner, der sich etwa über einen Mailanhang auf dem PC eingenistet hat, kann unbemerkt Daten senden, auch wenn der Firewall das Empfangen von Daten verhindert. Lediglich die Datei Pfirewall.TXT, die auf Wunsch sämtliche Netzwerkzugriffe protokolliert, ermöglicht einen detaillierten Einblick in sämtliche Netzwerkzugriffe.

Für Heimanwender, deren Rechner in kein lokales Netzwerk integriert ist, bietet die Firewall-Funktion einen gewissen Schutz. Bedienung und Konfiguration sind allerdings

schlichtweg eine Zumutung und erfordern mindestens einen Grundkurs in Sachen Netzwerktechnik.

Ich hoffe einen kleinen Überblick über die Momentane Sicherheitssituation gegeben zu haben und wünsche euch ein Sicheres PC-Vergnügen.