

Security bei Webanwendungen

Fachbereichsarbeit im Wahlpflichtfach Informatik

Christian Andreas Feigelbinder

Betreuer.

Mag. Carl Metnitz

GRG I Stubenbastei
Stubenbastei 6-8, 1010 Wien

Schuljahr 2003/2004

Wien, 14. Februar 2004

Inhaltsverzeichnis:

1.	Vorwort	4
2.	Computer Security	6
2.1	Was ist Computer Security?	6
2.2	Warum ist Computer Security wichtig?	6
2.3	Von wem geht Gefahr aus?	8
3.	Gefahrenpotenziale erkennen	10
3.1	Viren, Würmer und Trojanische Pferde	10
3.1.1	Viren	11
3.1.1.1	Dateiviren	12
3.1.1.2	Bootviren	14
3.1.1.3	Scriptviren	15
3.1.1.4	Makroviren	16
3.1.1.5	Begleiterviren	17
3.1.1.6	Strategien von Viren	17
3.1.2	Würmer	18
3.1.3	Trojanische Pferde	19
3.2	DoS-Attacken	20
3.3	IP-Spoofing/Web-Spoofing	21
3.4	Trittbrettfahrer	22

4.	Systemlandschaften im Überblick	23
4.1	Firewall	23
4.2	Proxy-Server	27
4.3	Virens Scanner	28
4.4	Router	29
5.	Securitymaßnahmen setzen	30
5.1	Aufstellen eines Sicherheitskonzeptes	30
5.2	Tipps für die sichere Anwendung von Outlook	30
5.3	Richtige Konfiguration des Internet Explorers	31
5.4	VBS- und JS-Schädlingen das Handwerk legen	34
5.5	Der richtige Umgang mit Makros bei Office	36
5.6	Nicht als Administrator arbeiten	37
5.7	Regelmäßige Updates durchführen	37
5.8	Kryptographie	38
5.9	Ports sperren	40
5.10	Was tun wenn es brennt?	41
6.	Conclusio	44
7.	Quellenverzeichnis	45

1. Vorwort

Als ich im Sommer 2003 begonnen habe, mich mit dem Thema Sicherheit zu beschäftigen, hätte ich es nicht für möglich gehalten, dass dieses Thema dermaßen weitreichende Konsequenzen besitzt. Je mehr Literatur ich studierte, desto selektiver musste Grundsätzliches zum Thema gefiltert werden, um die Fachbereichsarbeit auf das Wesentliche zu beschränken. In dieser Arbeit habe ich einen Gesamtüberblick über Sicherheitsaspekte im Internet erstellt.

Während der Ausarbeitung der Fachbereichsarbeit gewann das Thema Security neue Aktualität. Durch das Auftreten des Wurms MyDoom hat sich deutlich gezeigt, wie eminent wichtig Sicherheitsvorkehrungen sind. Plötzlich berichten alle Medien über die Sicherheitsprobleme, die weltweit enormen Schaden verursachen. Schätzungsweise werden monatlich 400 neue Schädlinge freigesetzt, mit unterschiedlichem Gefahrenpotenzial.

Darüber hinaus soll das Bewusstsein der privaten Internetuser für Websecurity geschärft werden. Es werden Ansätze für einfache Sicherheitsmaßnahmen behandelt. Grundsätzlich gilt, dass Präventivmaßnahmen wirtschaftlicher als Reparaturmaßnahmen im Ernstfall sind.

Die Zielgruppe meiner Fachbereichsarbeit ist die Windows-Welt. Jedoch sind die dargestellten grundlegenden Prinzipien auch für andere Betriebssysteme und Anwendungen gültig.

Die Ausführungen sind für ambitionierte PC-User leicht verständlich, daher ist kein Spezialwissen erforderlich. Wer die Grundzüge beachtet, wird die Katastrophenmeldungen der Presse richtig beurteilen und den durch Angreifer geplanten Schaden auf seinem Rechner präventiv verhindern.

2. Computer Security

2.1 Was ist Computer Security?

Computer Security ist ein Überbegriff für alle Verfahren und Einrichtungen, die einen ausreichenden Schutz für User und Maschine zum Ziel haben. Unter einem „ausreichenden Schutz“ versteht man, dass weder ein Angreifer von außen noch von innen (zum Beispiel Mitarbeiter eines Unternehmens) unerlaubterweise Zugriff auf den eigenen Rechner¹ und/oder damit auch auf sensiblen Daten erhält.

2.2 Warum ist Computer Security wichtig?

Gerade heute ist es wichtiger denn je, sich zu schützen: Denn jährlich steigt die Anzahl von neuen Viren, Würmern, neuen Varianten alter Viren und im weiteren Sinne auch die Gefahr von diesen befallen zu werden explosionsartig an. Hinzu kommt, dass die Hersteller der Antivirensoftware der Entwicklung und Verbreitung von Viren immer hinterherhinken. Allerdings ist leider kein Ende dieses Trends in Sicht. Außerdem sind die Zeiten lange vorbei, in denen nur große Konzerne und staatliche Stellen das Ziel derartiger Angriffe waren.

¹ Ein Synonym für Computer

Mittlerweile existieren zahlreiche Hobbyhacker, die nicht das Know-How besitzen, sondern nur noch fertige aus dem Internet heruntergeladene „Hackertools“² verwenden.

Diese Entwicklung wird aufgrund der leichten Beschaffung solcher Programme und der relativ leichten Handhabung forciert. Eine weitere Konsequenz dieses Trends ist, dass nun Privatpersonen einfach aus Spaß gehackt³ werden, weil diese in der Regel entweder gar nicht oder nur unzureichend geschützt sind. Es darf aber nicht außer Acht gelassen werden, welche weitreichenden Folgen ein schlechter bzw. nicht vorhandener Schutz hat. Ein gutes Beispiel geben jene Würmer ab, die sich selbst durch Massenmails verbreiten. Durch diese Vorgehensweise sind in kürzester Zeit tausende Computer infiziert, die wiederum weitere Rechner verseuchen. Dieser „Teufelskreis“ wird erst durch ein Update⁴ der Virens Scanner, die Verwendung eines Remover⁵ und dem sprichwörtlichem „Stopfen der Sicherheitslücke“ unterbrochen. Der verursachte Schaden solcher Viren bzw. Würmer ist, wie die Vergangenheit gezeigt hat, allein in Österreich enorm.

Zusammenfassend ein kurzer Überblick warum Computer Security und in weiterer Folge ein umfassender Schutz wichtig ist:

- Explosionsartiger Anstieg von neuen Viren und Würmern
- Privatpersonen sind vermehrt Ziel von „Möchtegernhacker“
- Enormer Schaden durch Missbrauch von Daten

² Programme mit denen man andere angreifen kann ohne selbst das Hintergrundwissen zu haben, wie diese funktionieren

³ hacken ist ein Synonym für angreifen bzw. sich Zugriff auf einen anderen Computer zu verschaffen

⁴ dt. Aktualisierung

⁵ Ein Tool zur Entfernung jeglicher Spuren eines Virus/Wurms

2.3 Von wem geht Gefahr aus?

Im Allgemeinen kann man die Angreifer in 3 verschiedene Gruppen einteilen.

- Hacker
- Cracker
- Scriptkiddies („Möchtegernhacker“)

Die beiden ersteren sind annähernd identisch, doch werden sie an Hand ihrer Motive unterschiedlich bezeichnet. Unter anderem auch deswegen weil die „legalen“ Hacker sich von den kriminellen Aktivitäten ihrer Konkurrenten abgrenzen wollen. Der grobe Unterschied zwischen diesen liegt darin, dass die „legalen“ Hacker im Gegensatz zu Cracker eine Hackermoral besitzen, die unter anderem besagt:

„Öffentliche Daten nutzen, private Daten schützen.“⁶

Oft brechen Hacker nur deswegen in ein System ein, um dann anschließend die gefundene und benutzte Sicherheitslücke offen zulegen und um die Softwarefirmen zu zwingen bessere Sicherungsverfahren zu entwickeln.

In weiterer Folge arbeiten Hacker auch als Sicherheitsberater für Firmen. Allerdings sei erwähnt, dass die von ihnen durchgeführten sog. „Penetrationstests“ nur Unsicherheiten und niemals Sicherheit aufzeigen können.

⁶ www.ccc.de/hackerethics Chaos Computer Club

Wie schon angedeutet verbindet man mit Cracker Personen, die entweder aus Profitgier oder auch aus Langeweile mutwillig anderen Schaden zufügen, indem sie z.B. sich in deren Computer reinhacken, Daten manipulieren, sabotieren bzw. kopieren und verkaufen.

Von den Motiven her sind Scriptkiddies ähnlich den Crackern, mit dem Unterschied, dass sie fertig programmierte Hackertools verwenden ohne auch nur einen blassen Schimmer zu besitzen, wie diese funktionieren und welchen Schaden sie anrichten. Für sie ist das „Hacken“ lediglich eine gewöhnliche Freizeitaktivität.

3. Gefahrenpotenziale erkennen

Bevor man eine effektive Sicherheitsrichtlinie erstellen kann, ist es unbedingt erforderlich, dass man über die Gefahren und Risiken Bescheid weiß, die jeden User bzw. deren Computersystem/e bedrohen. Es gibt bekanntermaßen eine weitreichende Palette von Möglichkeiten wie ein Angreifer in ein System einbrechen und/oder es beeinträchtigen kann.

In diesem Kapitel werden einige geläufige Angriffe bzw. Gefahren erläutert:

3.1 Viren, Würmer und Trojanische Pferde

Man bezeichnet Viren, Würmer und Trojanische Pferde auch als „Malware“⁷, da sie (fast) immer eine schädliche Funktion haben. Viren und Würmer sind bis auf die Verbreitung identisch. Denn Viren werden passiv und Würmer aktiv übertragen. (Siehe Kapitel 3.1.1 und 3.1.2)

⁷ sinngemäß übersetzt: schädliche Ware

3.1.1 Viren

Computerviren⁸ sind kleine Programme, die sich von selbst replizieren⁹ und eventuell Dateien oder Systembereiche verändern bzw. schädigen.

Die Verbreitung wird durch die Infektion eines so genannten Wirtsprogrammes¹⁰ und der unbewussten Hilfe des Users bewerkstelligt. Ein Virus erreicht dies, indem er eine Kopie von sich selbst mit dem Programm oder dessen Umgebung fix verankert. Für den Benutzer ist dieser Prozess völlig unsichtbar. Das bedeutet, dass der Virus unentdeckt bleibt, sich ungestört vermehren und verbreiten kann.

Primär gilt ein Programm bereits dann als Virus, wenn es sich reproduzieren und andere Applikationen befallen kann. Zusätzlich kann der Virus noch beliebige Aktionen durchführen, die in der Regel einen Schaden verursachen.

Grundsätzlich kann man Viren in 5 Kategorien einteilen:

- Dateiviren
- Scriptviren
- Bootviren
- Makroviren
- Begleiterviren

Außerdem gibt es so genannte Alleskönner, die auch als multipartite Viren bezeichnet werden.

⁸ vergleichbar mit dem biologischem Pendant

⁹ Synonym von reproduzieren

¹⁰ Ein beliebiges Programm, das nach der Ansteckung einen Virus beherbergt

Ein solcher Virus ist in der Lage mehrere Dateitypen zu infizieren und verschiedene Funktionen auszuführen – wie zum Beispiel ein Bootvirus, der auch Microsoft Office-Dokumente befällt. Weiterhin nennt man Viren, die unabhängig vom Betriebssystem agieren, Multiplattform-Viren. Allerdings benötigen die Autoren von solchen komplexen Viren immer das Know-How der jeweiligen Gebiete, die sie als Ziel vorsehen.

Eine weitere Möglichkeit mehrere Ziele gleichzeitig anzugreifen ist, wenn ein Virus einen anderen aussetzt. Hierbei spricht man dann von einem Dropper.

So makaber es auch klingen mag: Dem Virenautor sind aufgrund der unzähligen Kombinationsmöglichkeiten keine Grenzen gesetzt.

3.1.1.1 Dateiviren

Dateiviren sind jene Viren, die eine Kopie von sich selbst in Programmdateien¹¹ kopieren. Es gibt je nach Betriebssystem verschiedene Typen von Programmdateien.

Beispielsweise gibt es in DOS¹² und Windows¹³ folgende 3 Arten von Programmdateien, wobei Windows noch viele mehr kennt:

- Com-Dateien

¹¹ Eine Programmdatei ist eine ausführbare Datei, die Befehle enthält, welche beim Aufruf nach und nach ausgeführt werden

¹² DOS ist das Betriebssystem von Microsoft, das bis in die Mitte der 90er am weitesten verbreitet war

¹³ Sammelbezeichnung von verschiedenen Betriebssystemversionen von Microsoft; beinhaltet Windows 95, 98, ME, 2000, XP

- Exe-Dateien
- Bat-Dateien

Dateiviren haben mehrere Möglichkeiten ein Programm zu infizieren. Je nachdem ob der Virus das Wirtsprogramm von Anfang an überschreibt – und dabei riskiert, dass es nicht mehr funktioniert – oder seinen Programmcode lediglich einfügt, spricht man von einem überschreibenden oder nicht überschreibenden Virus. Bei der zweiten Variante fügt der Virus seinen Code entweder vor, dazwischen oder nach dem eigentlichen Programmcode des Wirtsprogramms ein. Natürlich muss der Virus dann bei Bedarf dafür sorgen, dass er mittels Sprungbefehle als erstes gestartet wird. Da er nur so für eine ausreichende Verbreitung sorgen kann. Ansonsten ist diese eher dem Zufall überlassen.

Ein Virus hat nach seiner Aktivierung die Möglichkeit sich in den Arbeitsspeicher zu transferieren. Dies erreicht er unter DOS durch die Verwendung des TSR-Befehls¹⁴. Deswegen nennt man solch einen Virus einen residenten Virus bzw. TSR-Virus. Bei den aktuelleren Betriebssystemen hat er mittlerweile viel mehr Möglichkeiten sich zu tarnen. Wie zum Beispiel als Systemtreiber¹⁵ oder auch als Prozess¹⁶ mit einem unsichtbaren Fenster. Auf diese Weise bleibt der Virus auch nach Beendigung des Wirtsprogramms aktiv und wird erst durch einen Neustart des Computers beendet. Schlaue Virenautoren lassen aber ihre Viren wichtige Programmdateien des Betriebssystems infizieren, sodass diese bei

¹⁴ Abkürzung für **T**erminate and **S**tay **R**esident

¹⁵ Treiber werden beim Start automatisch geladen und werden für den Betrieb von allen Hardwarekomponenten benötigt – wie zum Beispiel der Grafikkarte

¹⁶ Ein Prozess wird auch als Task bezeichnet; gemeint sind laufende Programme

jedem Start automatisch aufgerufen werden. „Vorteil“ dieser Prozedur ist, dass es um einiges schwieriger ist, den Virus zu entfernen als unter normalen Umständen. Außerdem wird es dem Virus sehr leicht gemacht weitere Programme zu finden und sie dann anschließend zu befallen.

Beispiele für Dateiviren sind die sehr destruktiven „Magistr“, „Kriz“ und „CIH“.

3.1.1.2 Bootviren

Um die Funktionsweise von Bootviren zu verstehen ist ein kurzer Exkurs über den Aufbau von Disketten und Festplatten notwendig: Jede Diskette besteht aus vielen verschiedenen Sektoren, von denen der erste der Bootsektor ist. Dieser Bootsektor enthält entweder ein Programm, das den weiteren Verlauf des Bootens¹⁷ bestimmt, oder eine Fehleroutine, die dem User erklärt, dass sich die Diskette nicht zum Booten eignet. Eben dieses Verhalten nutzen Bootviren aus, indem sie sich an deren Stelle setzen. So kann der Rechner mühelos infiziert werden, wenn der Computer mittels einer infizierten Diskette oder CD hochgefahren wird.

Der eigentliche „Vorteil“ von Bootviren besteht darin, dass der Virus aktiv werden kann bevor ein Antivirenprogramm gestartet wird.

Nachdem der Virus aktiviert wurde, versucht er die Festplatte zu infizieren, um in Zukunft auch ohne dem Booten mit der verseuchten Diskette oder CD automatisch gestartet zu werden.

¹⁷ Hochfahren bzw. Starten des Computers

Um sein Ziel, die Infizierung von bis jetzt nicht infizierten Disketten zu bewerkstelligen, bleibt der Virus immer resident im Arbeitsspeicher. Er kann somit bequem bei jedem Zugriff auf eine Diskette – sei es ein Kopiervorgang oder auch nur ein Lesezugriff – diese sofort infizieren. Es sei denn der Schreibschutz der Diskette ist aktiviert.

Bootviren waren vor allem in der Zeit weit verbreitet als Daten (hauptsächlich) über eine Diskette von einem Computer auf den anderen übertragen wurden. Heutzutage wurden sie von Script-, Makroviren und (Mail-) Würmern abgelöst.

Einige der bekanntesten Bootviren sind „Michelangelo“, „Monkey“ und „Brain“.

3.1.1.3 Scriptviren

Scriptviren sind Viren, die beispielsweise in VisualBasic Script (VBS) oder in JavaScript geschrieben sind. Sie zeichnen sich im Gegensatz zu anderen Programmiersprachen wie zum Beispiel Assembler¹⁸ durch eine vereinfachte Programmierung und Handhabung aus. Ein typischer Vertreter für Scriptviren ist zum Beispiel „Rabbit“.

¹⁸ Eine maschinenorientierte Programmiersprache

3.1.1.4 Makroviren

Makroviren gibt es seit der Einführung und Verbreitung von „Word“, einem Textverarbeitungsprogramm von Microsoft. Dieses Programm nutzt erstmals Makros, weil diese unzählige automatisierte Aufgaben erfüllen und deshalb bei vielen Programmvorgängen eingesetzt werden können.

Man verwendet sie zum Beispiel um so genannte „Shortcuts“¹⁹ zu realisieren. Die meisten Makroviren befallen hauptsächlich Dokumente, die mit verschiedenen Microsoft Office-Produkten erstellt werden, da diese sehr weit verbreitet sind. Makroviren unterscheiden sich von den herkömmlichen Makros nur durch die Schädigungsfunktion, die sie beinhalten. Das heißt rein formal ist ein Makrovirus nicht zu entdecken. Nur beim Ansehen des Quellcodes, ist es möglich ihn aufzuspüren und selbst das funktioniert nicht immer, weil es doch einige Viren gibt, die versuchen ihren Code zu verstecken.

Makros werden – ebenso auch Makroviren – zusammen mit dem Text des Dokuments mitgespeichert und dadurch auch mit Hilfe des Users weitergegeben. Um aus der Sicht des Virus eine ausreichende Verbreitung zu gewährleisten, versucht er nach seiner Aktivierung das Programm so zu manipulieren, sodass er bei jedem Programmstart automatisch gestartet wird und er dadurch nicht so leicht entfernt werden kann.

¹⁹ Ein Befehl, der nicht durch das Menü aufgerufen wird, sondern durch eine Tastenkombination. Bekannte Shortcuts sind zum Beispiel STRG + C, STRG + V. Diese repräsentieren die Befehle kopieren bzw. einfügen.

3.1.1.5 Begleiterviren

Begleiterviren, auch Companion-Viren genannt, sind Viren, die nicht das Programm selbst befallen, sondern deren Umgebung. Das heißt sie benutzen eine Reihe von Tricks damit sie an Stelle des Programms gestartet werden. Begleiterviren sind kaum verbreitet, da sie für jedes Programm eine eigene Falle brauchen.

3.1.1.6 Strategien von Viren

Das Ziel eines Virus ist es immer sich unbemerkt zu vermehren und erst dann entdeckt zu werden, wenn es der Virenautor vorsieht. Das erreicht dieser durch die Implementierung von „Trigger“. Trigger beinhalten die Parameter, die für die Auslösung der Schadfunktion relevant sind. Selbst die destruktivsten Viren wie „CIH“ bleiben einige Zeit harmlos und versteckt bevor sie ihre Schadfunktionen ausführen. Um eine Entdeckung zu verhindern, stehen einem Virus mehrere Maßnahmen und Strategien zur Verfügung, die im folgenden kurz erläutert werden:

Viren sind in der Lage die Dateiattribute²⁰ – wie Erstelldatum bzw. das Datum des letzten Zugriffs, Größe der Datei oder ob eine Datei versteckt ist – von befallenen Dateien zu manipulieren. Außerdem bedienen sich viele Viren der „Tarnkappenstrategie“. Das bedeutet, dass sie versuchen dem Anwender eine unberührte und völlig intakte Systemlandschaft vorzutäuschen. Ebenso die Verschlüsselung des Virencodes bietet die potentielle Chance verborgen zu bleiben. Jedoch ist es den heutigen

²⁰ Dateiattribute stellen die Eigenschaften einer Datei dar.

Virensclannern möglich, sie trotzdem aufzuspüren. (Siehe Kapitel 4.3 Virensclanner)

Allerdings wird es schwieriger, wenn es sich um einen polymorphen²¹ Virus handelt. Denn dieser erreicht zum Beispiel durch die Anwendung verschiedener Verschlüsselungen eine Vielzahl von möglichen Gestalten.

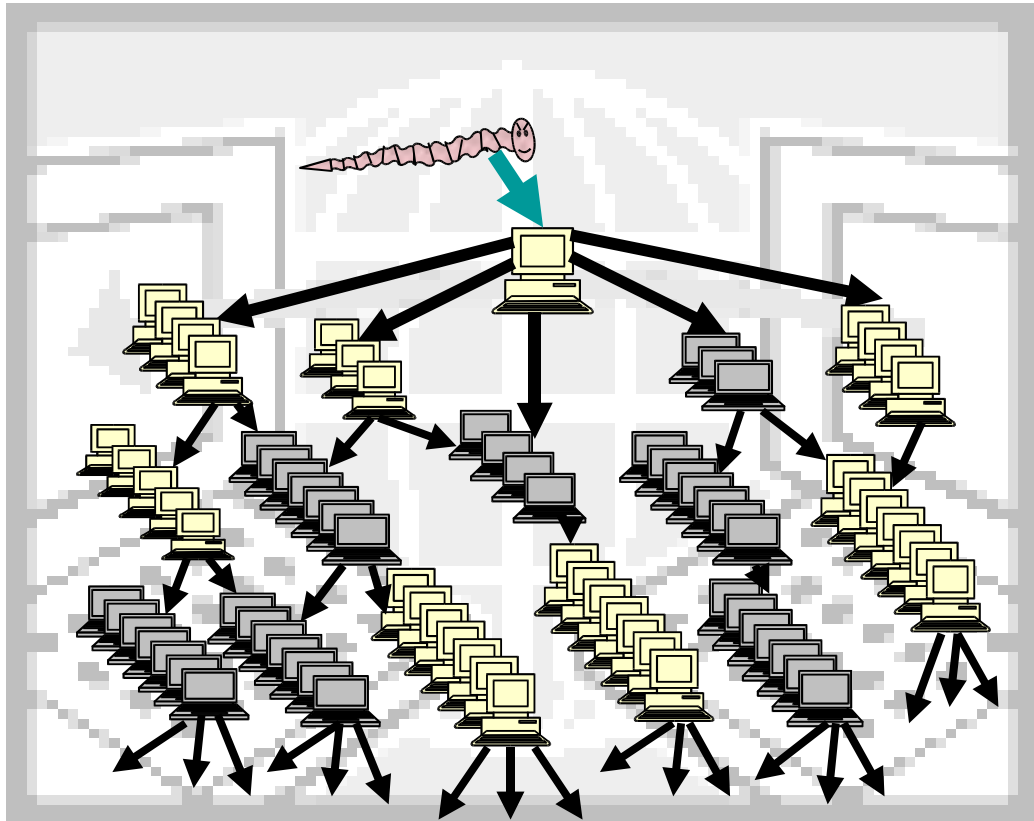
3.1.2 Würmer

Würmer sind - wie vorhin erwähnt - nahezu identisch mit Viren. Jedoch verlassen sie sich nicht auf die „Schützenhilfe“ des Users, sondern übernehmen selbst ihre Verbreitung, indem sie sich zum Beispiel auf einen anderen Computer kopieren. Je nach Art der Verbreitung nennt man sie entweder Internet-, Mail- oder LAN-Würmer²².

Speziell hervorzuheben sind Mailwürmer, da diese in letzter Zeit sehr verbreitet sind. Ein solcher „Mass-Mailer“ ist beispielsweise der zuletzt aufgetauchte „MyDoom.A“ bzw. die B-Variante „MyDoom.B“.

²¹ Kommt aus dem griechischen (polymorphos) und bedeutet vielgestaltig.

²² LAN ist die Abkürzung von **L**ocal **A**rea **N**etwork und steht für ein lokales Computernetzwerk



Mass-Mailer - I-Worm infiziert Computer 1, breitet sich automatisch aus



= Laptop



= Desktop

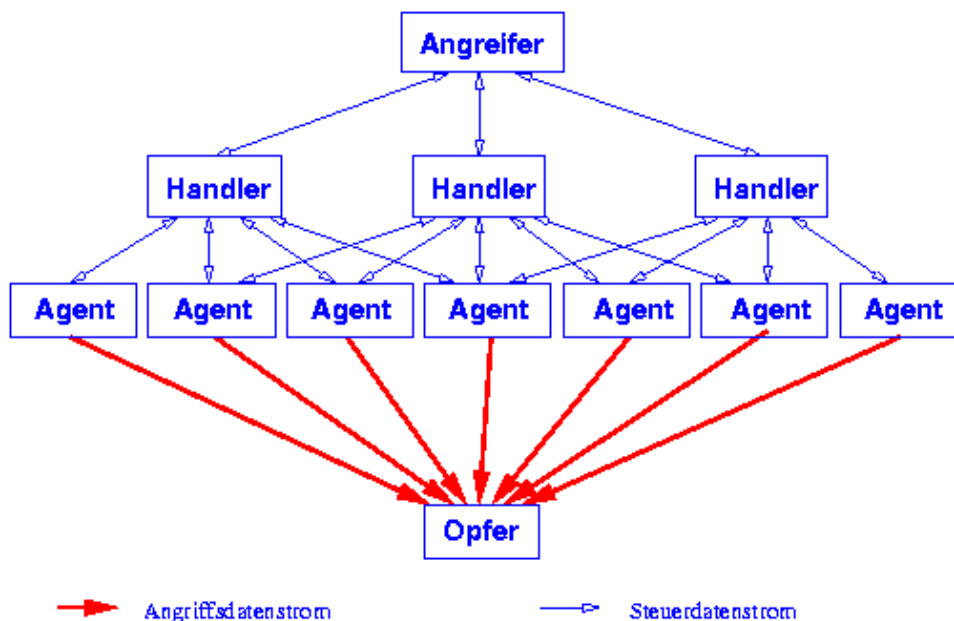
3.1.3 Trojanische Pferde

Unter einem „Trojaner“ versteht man ein Programm, das nicht in der Lage ist sich selbst zu verbreiten - wie es bei Viren oder Würmern der Fall ist - , aber verschiedene schädliche Aktionen durchführt. In der Regel werden Trojaner benutzt um den Computer des Opfers auszuspionieren oder gar zu übernehmen. Sie sind vor allem deswegen gefährlich weil sie sich als harmlose Anwendungen tarnen. Außerdem treten sie häufig in Kombination mit einem Virus oder Wurm auf.

3.2 DoS-Attacken

Unter einer **D**enial **o**f **S**ervice Attacke (kurz DoS) versteht man einen Angriff, dessen Ziel es ist, einen bestimmten Computer bzw. Server lahm zulegen.

Im Erfolgsfall verweigert das Computersystem völlig seinen Dienst. Es gibt mehrere Möglichkeiten dies zu bewerkstelligen. Die simpelste Methode ist das System so mit Verbindungsanforderungen zu bombardieren, sodass der Computer nur noch mit sich selbst beschäftigt ist. Folgerichtig ist es dem User dadurch nicht mehr möglich irgendwelche Applikationen durchzuführen. Aufgrund der mangelnden Anonymität des Angreifers existiert mittlerweile eine neue Verfahrensweise, die „DDoS“ oder „**D**istributed **D**enial **o**f **S**ervice“ genannt wird. Bei dieser Form des Angriffs wird der Rechner von einer Vielzahl von Computern angegriffen.



Schematische Darstellung eines DDoS Angriffs

3.3 IP-Spoofing/Web-Spoofing

Generell versteht man unter „Spoofing“ das Vortäuschen einer nicht vorhandenen Begebenheit. Ein „Spoofing-Angriff“ kann in unterschiedlicher Weise auftreten:

Beispielsweise wenn ein Angreifer Daten (Datenpakete) verschickt, ohne dass seine echte IP-Adresse angezeigt wird, sondern eine gefälschte verwendet, dann spricht man von „IP-Spoofing“ oder auch „IP-Maskerade“. Durch diese Vorgehensweise erreicht der Angreifer eine gewisse Anonymität, da man diese Daten nicht zu ihm zurückverfolgen kann.

In weiterer Folge ist es ihm zum Beispiel möglich in Kombination mit Password-Snooping²³ eine Identität vorzutäuschen, um entweder an sensible Informationen zu gelangen oder gar Aktionen auszuführen für die er nicht autorisiert ist. Ebenso gibt es die Möglichkeit „Web-Spoofing“ zu betreiben.

Bei dieser „Attacke“ erstellt der Angreifer eine Kopie einer Website und versucht dann seine Opfer auf eben diese zu locken. Dadurch kann zum Beispiel ein Virus oder Trojaner deren Systeme infiltrieren. Allerdings könnte er so auch versuchen vertrauliche Daten zu erbeuten – wie Kreditkartennummer, Telefonnummer, Name, Adresse, etc. Ein weiteres Merkmal von Web-Spoofing ist, dass man der angezeigten Adresse in der Adressenleiste nicht vertrauen kann, da diese leicht gefälscht werden kann.

²³ Password-Snooping ist ein Verfahren, in dem man eine IP-Adresse und ein Passwort, das für eine Freischaltung eines Dienstes benötigt wird, abhört.

3.4 Trittbrettfahrer

Unter Trittbrettfahrer versteht man Angreifer, die einen Verbindungsaufbau verfolgen, um sich unbemerkt an Authentifikationsverfahren – einschließlich kryptographischen – vorbeizumogeln. Nach erfolgreichem Verbindungsaufbau blockt der Angreifer den Computer des ausgenutzten Opfers so ab, sodass für diesen die Verbindung abgebrochen ist.

„Nun kann der Angreifer die authentifizierte Verbindung als Trittbrettfahrer für sich und seine Ziele nutzen.“²⁴

Es gibt eine Vielzahl von Schadprogrammen und möglichen Angriffsarten, deren Erwähnung die Kapazität dieser Arbeit zweifellos sprengen würden.

²⁴ Firewallsysteme – Sicherheit für Internet und Intranet, Norbert Pohlmann; B.S. 79

4. Systemlandschaften im Überblick

In diesem Kapitel werden einige Soft- bzw. Hardwareprodukte beschrieben und erläutert, die hinsichtlich eines umfangreichen Computerschutzes vorteilhaft wären.

4.1 Firewall

Eine Firewall²⁵ ist eine Vorrichtung, die unerwünschte Zugriffe, Datenströme – unabhängig davon, ob sie von außen oder innen kommen – abblockt und daher vollkommen unterbinden soll. Grundsätzlich besteht eine Firewall entweder aus einem „Application Gateway“²⁶, einem „Packet Filter“ oder einer Kombination aus beidem. Rein technisch gesehen gibt es viele Kombinationsmöglichkeiten, da durchaus mehrere Application Gateways und Packet Filter hintereinander geschaltet werden können. Die gewünschten Sicherheitsrichtlinien werden durch ein Security Management umgesetzt, das alle anderen Firewall-Elemente kontrolliert und verwaltet.

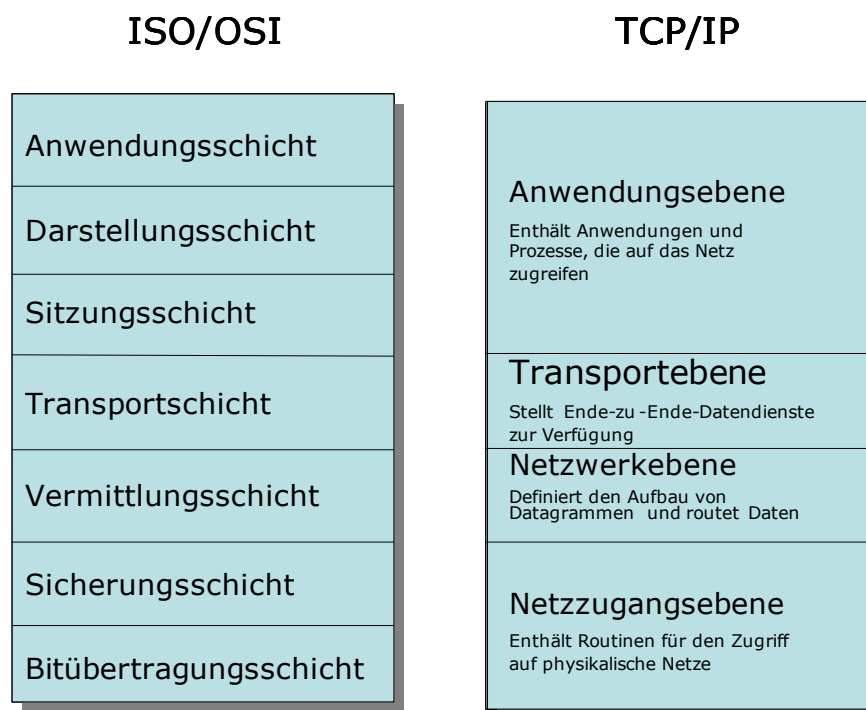
²⁵ dt. Brandschutzmauer

²⁶ Stellt eine Schnittstelle zwischen internen Netz (LAN) und externen Netz (Internet) dar; siehe „Common Point of Trust“ Seite 26

Um zu verstehen, wie die beiden Hauptkomponenten funktionieren, ist es nötig das ISO/OSI-Referenzmodell²⁷ zu kennen:

Das Modell besteht aus 7 Schichten, wobei jede Ebene nur die für sie festgelegte Funktion ausführt. In weiterer Folge ist es einleuchtend, dass bei einer Verbindung zwischen zwei Computern nur die Daten der jeweiligen gleichen Schicht verarbeitet werden können. So kann die Sitzungsschicht des zweiten Rechners nur die Daten auslesen und auswerten, welche die Sitzungsschicht des ersten Computers verschickt.

Überdies wird der Prozess durch die TCP/IP-Protokollarchitektur veranschaulicht.



Schematische Darstellung der beiden Modelle

²⁷ ISO steht für **I**nternational **O**rganisation for **S**tandardization. OSI bedeutet **O**pen **S**ystem **I**nterconnection.

Ein Packet Filter ist ein Modul, welches den Datenfluss von der Netzzugangs- bis zur Transportebene kontrolliert und protokolliert. Er ist zwar wegen der geringen Komplexität einfach zu realisieren, doch fehlen ihm die Möglichkeiten die Struktur des zu schützenden Netzwerks zu verbergen und Anwendungen zu überwachen, da er nur bis zur Transportebene protokolliert.

Diese Schwächen gleicht ein Packet Filter einerseits durch die Flexibilität für neue Dienste und andererseits durch eine tiefgreifende Analyse der Daten innerhalb seines Bereiches aus.

Im Gegensatz dazu arbeitet ein Application Gateway, welches sich ausschließlich auf die Anwendungsebene beschränkt. Weiters kann es das LAN vom Internet sowohl logisch als auch physikalisch entkoppeln. D.h. im Notfall kann es symbolisch gesehen den „Stecker“ ziehen.

Zusätzlich unterscheidet man zwischen einem Single-homed und einem Dual-homed Gateway. Der Unterschied besteht darin, dass das Dual-homed mit 2 Netzwerkanschlüssen arbeitet und daher die volle Kontrolle über die Datenpakete hat. Bei der Single-homed Variante gibt es lediglich nur einen Anschluss. Jedoch besteht dann das Risiko, dass ein Angreifer das Application Gateway umgeht. Zusätzlich verwendet es Proxies, die je nach Art des Proxy unterschiedliche Dienste kontrollieren und überwachen. (Siehe Kapitel 4.2 Proxy-Server)

Grundsätzlich soll eine Firewall den bzw. die zu schützenden Computer vom unsicheren Netz, also Internet, abschirmen. Insofern soll es einem potenziellen Angreifer nicht möglich sein, festzustellen, wie viele Computer im LAN vorhanden sind - unabhängig davon, ob es nur einen oder mehrere gibt.

Vom Sicherheitsstandpunkt aus, soll sie den sog. „Common Point of Trust“ verwirklichen. D.h. es gibt keine anderen Möglichkeiten eine Verbindung zum Internet aufzubauen als über die Firewall.

Es gibt 2 Arten von Firewalls:

- Hardwarefirewalls
- Softwarefirewalls

Hardwarefirewalls sind in sich abgeschlossene Systeme, die zwischen dem Computer und dem Modem – sei es DSL, ISDN, oder analoges Modem - geschaltet werden. Durch die Unabhängigkeit vom zu schützenden Computer kann kein Softwarekonflikt entstehen. So gesehen können sie sich völlig auf ihre Arbeit, Hackerangriffe abblocken, konzentrieren.

Softwarefirewalls, oder auch Desktopfirewalls, sind im Gegensatz zu Hardwarefirewalls abhängig von ihrer Umgebung. D.h. es kann ohne weiteres passieren, dass die Firewall durch einen eingeschleppten Virus „abgeschossen“ werden kann. In so einem Fall ist die Sicherheit des Computers überhaupt nicht mehr gewährleistet. Ein Vorteil gegenüber den Hardwaremodellen besteht darin, dass sie besser gegen Trojaner und Spyware-Attacken schützen²⁸ können.

Doch einen zuverlässigen Schutz erreicht man nur durch eine Kombination:

„Sicherer Schutz vor Hacks, Trojanern und Malware ist nur möglich wenn der Anwender Desktop- und Hardwarefirewall kombiniert.“²⁹

²⁸ Wie gut eine Firewall vor Trojaner und Spyware tatsächlich schützt, variiert zwischen den unterschiedlichen Anbietern teilweise beträchtlich.

²⁹ PC Professionell, Nr. 3 Februar 2004, Seite 119, Konstantin Breyer

Allerdings sollte man nicht vergessen, dass man Sicherheit nicht durch das bloße Installieren erlangt, sondern dass es erforderlich ist die Firewall gut zu konfigurieren. Ein Scheinschutz ist fast ebenso schlimm wie gar kein Schutz.

4.2 Proxy-Server

Ein Proxy-Server fungiert als Stellvertreter zwischen dem User und dem Internet. Er kann ein Dienst im Internet, ein eigener Server, auf dem die entsprechende Software läuft, oder Bestandteil einer Firewall sein. Bei einer HTTP-Anfrage dient er als Webseitenspeicher, d.h. er sendet die gewünschte Seite an den Benutzer, sofern sie vorhanden ist. Ansonsten leitet er die Anfrage an den zuständigen Webserver weiter. Die Vorteile eines Proxy-Servers bestehen aus den mitunter beschleunigten Webseitendarstellungen und der zusätzlich gewonnenen Anonymität für den User, da der Webserver einer Seite lediglich mit dem Proxy-Server und nicht mit dem Anwender selbst kommuniziert. Zusätzlich ist er in der Lage eine Filterfunktion auszuführen, um bestimmte Webseiten zu verbieten. Ebenso kann er die Nutzung von Java Scripts und ActiveX untersagen.

Ein möglicher Nachteil des Proxy-Servers ist, dass er teilweise veraltete Webseiten vermittelt. Dies kann bei häufig aktualisierten Seiten passieren. Neben der Verwendung bei HTTP, kann er auch bei FTP, Telnet und anderen Diensten eingesetzt werden.

4.3 Virens Scanner

Ein Virens scanner ist ein Programm, das nach infizierten Dateien sucht und dann versucht diese zu bereinigen. Jedoch hängt es vom Typ der Datei, der Leistungsfähigkeit des Virens scanners und dem Virus ab, ob die Datei im Erfolgsfall weiterverwendet werden kann. Oft hilft es nur die Datei zu löschen, da sie nicht „gerettet“ werden kann.

Es gibt viele verschiedene Virens scanner, die sich mitunter stark in Preis und Leistungsfähigkeit unterscheiden. Manche können lediglich die Festplatte scannen. Hingegen bieten die meisten zusätzlich sog. „Wächter“ an, die jede aufgerufene Datei nach Schädlingen scannen.

Aufgrund der Tatsache, dass die Programme unterschiedliche Suchroutinen besitzen, kann es durchaus mehr Sicherheit verleihen, wenn man 2 Antivirens scanner verwendet bzw. Antivirensoftware, die mit mehreren Such-Engines arbeitet. Doch sollte es auf jeden Fall vermieden werden mehr als einen Wächter gleichzeitig zu verwenden, da diese sich gegenseitig behindern würden.

Obwohl die Antivirenhersteller unterschiedliche Such-Engines haben, gibt es grundsätzlich einige Gemeinsamkeiten:

Die Scanner haben in ihrer Virendatenbank die verschiedenen Gestalten bzw. Muster der Viren, Würmer und Trojaner gespeichert. Beim Suchvorgang wird nun der Code der Dateien mit dem der Viren in der Datenbank verglichen. Bei einer Übereinstimmung wird dann eine Virenwarnung ausgegeben und je nach Einstellung des Virens scanners wird sofort mit der Bereinigung begonnen.

Weiters unterstützen Antivirenprogramme mehr oder weniger gut heuristische Verfahren, die durch sinnvolle Schätzungen und

Annahmen neue unbekannte Viren bzw. Abwandlungen aufspüren können. Solche Verfahren bewirken zwar keinen besonders sicheren Schutz gegen neue Varianten von Viren, Würmern und Trojanern, aber es ist trotzdem besser als keine Erkennungsmöglichkeit. Wichtig bei der Konfiguration des Scanners ist, auf jeden Fall alle Dateien zu scannen. Das Scannen dauert deswegen unter Umständen länger, allerdings muss einem die Sicherheit des Computers das wert sein.

Ein gewisses Manko der meisten Antivirens Scanner ist das gezielte Aufspüren und Entfernen von kostenverursachenden Dialern³⁰ und Spywareprogrammen³¹. Beispiele für Spyware sind „Cydoor“, „Gain“ und „Gator“. Deswegen ist es empfehlenswert Programme, wie zum Beispiel „Ad-Aware“, zu verwenden, die unerwünschte Programme finden und dann löschen.

4.4 Router

Ein Router ist eine Hardwarekomponente, mit der man ein kleines LAN aufbauen kann. Ebenso lässt sich mit herkömmlichen Routern erreichen, dass bis zu 4 Personen/Computer gleichzeitig eine Verbindung zum Internet aufbauen können. Sicherheitstechnisch relevant ist, dass sie mit einem Packet Filter ausgerüstet sind. Allgemein lässt sich aber sagen, dass Router wegen ihrer eigentlichen Aufgabe nur bedingt Schutz vor Hackerangriffen -

³⁰ Ein Dialer ist eine Einwahl-Software, die eine Internetverbindung über die Telefonnummer eines Mehrwertdienstes aufbaut. In der Regel findet man Dialer auf unseriösen Webseiten, die beispielsweise pornografische Bilder oder Softwareraubkopien anbieten.

³¹ Sind Programme, die ohne Wissen bzw. gegen den Willen des Benutzers Daten, wie die Konfiguration des Computers oder die Surfgeohnheiten des Users, ausspähen und an andere übermitteln.

vor allem vor denen, welche die Sicherheitsmaßnahmen selbst angreifen - bieten können.

5. Securitymaßnahmen setzen

5.1 Aufstellen eines Sicherheitskonzeptes

Der erste Schritt in Richtung „sicheres System“ ist, sich bewusst zu machen, dass dieses durchaus mit recht simplen Mitteln zu realisieren ist. Oft ist ein Computer nur aufgrund fehlender Userschulung oder Aufmerksamkeit unsicher.

Folgerichtig ist es sehr wichtig Userschulung zu betreiben und jegliche Unachtsamkeiten zu vermeiden.

Sicher klingt das Wort „Sicherheitskonzept“ äußerst komplex und nach besonders viel Arbeit, doch ist mit diesem nichts anderes gemeint, als dass man sich als User Gedanken darüber macht, wie und wobei man sich schützen kann/muss.

5.2 Tipps für die sichere Anwendung von Outlook

Die größte Gefahrenquelle geht zweifelsohne von E-Mails mit fragwürdigen Attachements aus. Die Mails an sich sind in der Regel bis auf wenige Ausnahmen harmlos, doch sollte es auf das tunlichste vermieden werden einen Anhang auszuführen, dessen Integrität man nicht kennt. Erste Anhaltspunkte, ob der Inhalt des Mails gefährlich ist oder nicht, liefert die Betreffszeile. Wenn sie zum Beispiel in einer fremden Sprache verfasst ist, explizit auffordert, dass man den Anhang öffnen soll, oder für den Absender ungewöhnliche Begrüßungen enthält dann sollte das Mail sofort gelöscht werden.

Selbst wenn das Mail von einer bekannten E-Mailadresse stammt, gibt es keine Garantie, dass es ungefährlich und sicher ist. Generell sollte man immer auf verdächtige Betreffszeilen, Mitteilungstexte und selbstverständlich auch Anhänge achten. Ein gewisses Maß an Misstrauen ist hier sicher angebracht. Weiters gibt es eine Windows-Voreinstellung, die bewirkt, dass Dateien im Mailanhang einen harmlosen Eindruck machen, obwohl sie in Wahrheit den Virus/Wurm aktivieren. Daher sollte man in einem beliebigen Explorer-Fenster (nicht Internet Explorer!) unter Extras | Ordneroptionen | Ansicht die Funktion „Dateinamenerweiterungen bei bekannten Dateitypen ausblenden“ ausschalten. Ebenso sollte auch die Mailvorschau deaktiviert werden, da es bei gewissen Mailwürmern für eine Aktivierung ausreicht.

5.3 Richtige Konfiguration des Internet Explorers

Eine gute Konfiguration des Browsers ist für sicheres surfen unumgänglich. Die hierzu notwendigen Einstellungen können bei IE 6 unter Extras | Internetoptionen | Sicherheit vorgenommen werden. Auf den ersten Blick sieht man, dass der Explorer mehrere Sicherheitszonen kennt, deren zugeordneten Websites unterschiedliche Rechte abhängig vom Sicherheitsniveau besitzen. Es empfiehlt sich die Einstellungen etwas anzupassen, da die Standardeinstellungen durchaus einiges Risikopotenzial bieten. Im Zuge dessen sollte die „Internet“ Zone mit Hilfe des Schiebereglers auf die Sicherheitsstufe „hoch“ gesetzt werden. Bei Bedarf kann es ebenso nicht schaden die Zone „Vertrauenswürdige Sites“ von „sehr niedrig“ auf „mittel“ hinaufzustufen.

Im großen und ganzen sollten die Einstellungen nun passen, doch kann man den Komfort erhöhen, indem man einige wenige für die Internetzone wieder etwas lockert:

Das dazu notwendige Fenster findet man unter „Stufe anpassen...“. Dort wird man unweigerlich mit vielen Auswahlmöglichkeiten konfrontiert, die größtenteils unberührt bleiben können. Wenn man nun hinunter scrollt, entdeckt man einen Unterpunkt namens „Dateidownload“.

Diese Option kann man ruhig auf „aktivieren“ setzen, da ohnehin bei einem Download ein eigenes Fenster erscheint, das den User fragt, was passieren soll. Ebenso ist es vertretbar, wenn man unter „Java-Einstellungen“ den Punkt „Hohe Sicherheit“ auswählt, da Java als eine sehr sichere Programmiersprache gilt. Eine weitere Option, die nützlich ist und keine hohen Risiken birgt, ist die Funktion „Meta Refresh“. Diese ermöglicht das automatische Weiterleiten von einer Internetseite zu einer anderen. Zusätzlich ist es äußerst praktisch unter dem Unterpunkt „Ziehen und Ablegen oder Kopieren und Einfügen von Dateien“ das sog. Drag&Drop bzw. Cut&Paste zu erlauben.

Anschließend fehlt nur noch die Aufteilung der Seiten in die verschiedenen Zonen. Um dann zum Beispiel eine Seite in die Zone „Vertrauenswürdige Sites“ zu verschieben, muss man lediglich auf „Sites...“ klicken und kommt sofort in das entsprechende Fenster.

Eine weitere für den Datenschutz wichtige Einstellung wird im Register unter „Datenschutz“ vorgenommen. Hier werden die Cookie-Einstellungen vorgenommen. Cookies an sich sind ungefährlich, jedoch können sie dazu verwendet werden die Surfgewohnheiten des Users zu speichern.

Es hängt vom jeweiligen User ab, ob er dies nun in Kauf nimmt oder nicht. Doch bevor man gleich alle Cookies sperrt, sollte man beachten, dass sie durchwegs auch Vorteile bieten. Oft trifft man sie bei Webseiten als Teil eines Logins an. Das heißt sie speichern den Benutzernamen und das Kennwort, damit der Benutzer diese nicht jedes Mal neu eingeben muss. Manche Seiten würden ohne Cookies nur eingeschränkt funktionieren, da man ohne sie nicht feststellen kann, ob jemand eingeloggt ist oder nicht. Einen guten Kompromiß erzielt man, wenn man unter „Erweitert...“ die automatische Cookiebehandlung aufhebt und stattdessen die Cookies von den Erstanbietern und die Sitzungscookies, das sind Cookies die beim Schließen des Browsers (beim Beenden der Sitzung) gelöscht werden, aktiviert. Allerdings sollten die von Drittanbietern gesperrt werden, weil diese aus der Sicht des Datenschutzes bedenklich sind.

Zusätzlich bietet der Internet Explorer eine Hinweisfunktion, an Hand dessen man feststellen kann, ob eine Seite seriös ist oder nicht. Angenommen man ist zum Beispiel auf einer Webseite eines Onlineanbieters gelandet und wird aufgefordert persönliche Daten abzuschicken. Hier reicht ein kurzer Blick auf die Statusleiste: Wenn dort ein geschlossenes Schloss abgebildet ist, dann bedeutet es, dass diese Seite zumindest eine Verschlüsselung verwendet, um die Sicherheit der Daten während des Transports zu gewährleisten. Weiters kann man sich durch einen Doppelklick auf das Schloss das Sicherheitszertifikat anzeigen lassen. Dieses Zertifikat ist außerdem ein Beweis, ob man sich tatsächlich auf der in der Adressenleiste angegebenen Seite befindet. So ist ein gewisser Schutz vor Webspoofing gewährleistet.



Schloss für die Anzeige einer Verschlüsselung

Wer jedoch der Meinung ist, dass IE und Outlook insgesamt zu viele Sicherheitslücken besitzen und Microsoft kaum was dagegen unternimmt, dem steht es frei auf alternative Browser und Mailprogramme - wie „Mozilla“, „Opera“, „Eudora“, „Thunderbird“ usw. - umzusteigen.

„Zum einen vergehen typischerweise mehrere Wochen oder gar Monate, bis Microsoft einen Patch dagegen bereitstellt. Bei Redaktionsschluss gab es beispielsweise immer noch keinen Patch für das im November veröffentlichte Problem in der showhelpfunktion, über das eine Webseite beliebige Dateien installieren und starten kann. Zum Anderen finden sich auch danach noch genügend Surfer, die diese Patches nicht installiert haben.“³²

5.4 VBS- und JS-Schädlingen das Handwerk legen

Man kann jegliches Risiko von Scriptviren/-würmer befallen zu werden minimieren, indem man den „Windows Scripting Host“ deaktiviert. Dadurch ist es möglich zu verhindern, dass schädlicher Programmcode³³ ausgeführt wird. Es gibt mehrere Möglichkeiten dies zu bewerkstelligen:

Einerseits ist es möglich den „Windows Scripting Host“ auf älteren Windowsbetriebssystemen wie Windows98 einfach zu deinstallieren.

³² c't 2004, Heft 3, Jürgen Schmidt, Seite 118

³³ Betrifft allerdings nur in JavaScript oder VisualBasic Script geschriebenen Code

Andererseits erreicht man die Deaktivierung auch unter diesem OS³⁴ durch das Umbenennen der Datei „Wscript.exe“ im Windowssystemordner in zum Beispiel „Wscript.bck“. Dadurch ist es sehr leicht möglich den WSH bei Bedarf wieder zu aktivieren. Bei Windows NT, 2000 und XP Professional kann man auch den Zugriff auf diese Datei verweigern, indem allen Benutzern das Lesen und Ausführen dieser Datei verboten wird. In das dazu notwendige Fenster kommt man, wenn man die Datei mit der rechten Maustaste anklickt und dann Eigenschaften | Sicherheitseinstellungen auswählt. Dabei ist es wichtig, dass man als Administrator eingeloggt ist.

Ebenso effektiv und um einiges eleganter ist ein kleiner Eingriff in die Registrierdatenbank.

Hierfür muss zuerst der Registrierungs-Editor mit dem Befehl „regedit“ im Menü „Ausführen“ gestartet werden. Prompt erscheint ein dem Windows-Explorer ähnliches Fenster. Nun doppelklickt man auf den Ordner „Hkey_Classes_Root“. Dadurch wird der Inhalt dieses Ordners gezeigt und man muss nur noch die Dateinamenserweiterung „.VBS“ bzw. „.JS“ in beispielsweise „.JS-“ bzw. „.VB-“ umbenennen. Bei dieser Art der Deaktivierung werden fremde Scripts lahm gelegt, doch eigene Scripts können problemlos weiterverwendet werden, da nur diese die passende Endung besitzen.

Es hängt vom jeweiligen User ab, welche Methode er benutzt, doch für diejenigen, die öfters VBS-Scripts verwenden, empfiehlt sich durchaus die zuletzt genannte.

³⁴ **O**perating **S**ystem = Betriebssystem

5.5 Der richtige Umgang mit Makros bei Office

Makros an sich haben durchaus ihre Daseinsberechtigung, doch sollte man vermeiden fremde Word-, Excel-, Powerpointdokumente aus unbekanntem Quellen vorschnell mit Office zu öffnen, weil dadurch leicht Makroviren aktiviert werden können.

Daher ist es ratsam, wenn man sie nur anschauen aber nicht bearbeiten will, sie mit einem Viewer³⁵ zu betrachten. Denn dort werden keine Makros verwendet und somit können eventuell vorhandene Makroviren nicht aktiv werden. Sollte es jedoch dennoch erforderlich sein, es mit dem jeweiligen Officeprodukt zu öffnen, dann empfiehlt es sich die Makrosicherheit auf die höchste Stufe zu stellen. Diese Maßnahme bietet zwar keinen 100%igen Schutz, aber sie sollte die meisten fremden Makros deaktivieren. Man findet diese Einstellung unter Extras | Makro | Sicherheit. Sollte es der Fall sein, dass es keinen solchen Eintrag gibt, ist es sehr wahrscheinlich, dass die Officeanwendung bereits verseucht ist.

Weiters sollte die Standardvorlage – wenn möglich gleich nach der Installation, um eine virenfreie Version zu garantieren – „Normal.dot“ separat gesichert werden, da sie bei Virenbefall verändert und damit nicht mehr sicher ist.

³⁵ Es gibt zahlreiche kostenlose Programme, die für das gefahrlose Betrachten diverser Dateiformate geeignet sind.

5.6 Nicht als Administrator arbeiten

Um zu verhindern, dass etwaige Würmer, Viren wichtige Systemdateien beschädigen oder überschreiben, Systemprozesse, wie beispielsweise eine laufende Firewall bzw. ein aktivierter Antivirens Scanner, beenden, ist es wichtig, dass man beim „normalen“ Arbeiten nicht als Administrator eingeloggt ist, sondern ein eigenes Benutzerprofil mit eingeschränkten Rechten verwendet. Bei den aktuellen Betriebssystemen ist es dann immer noch möglich Programme zu installieren, aber nur mit der Eingabe des korrekten Passworts. Obwohl die jetzigen Profilsysteme noch nicht besonders gut ausgereift sind, geht der Trend in Richtung komplexere und (hoffentlich) wirkungsvollere Sicherheitskonzepte.

5.7 Regelmäßige Updates durchführen

Die Verwendung eines Virens scanners und einer Firewall ist wichtig, doch ohne regelmäßige Sicherheitsupdates können sie auf keinen Fall ihre Schutzfunktion ausüben. Zu diesem Zweck haben die meisten Programme einen Internetupdater, mit dem man schnell und bequem die notwendigen Patches runterladen und installieren kann. Allerdings benötigt man auch die Service Packs und Hotfixes für das Betriebssystem und den Internet Explorer, da oft neue Sicherheitslücken gefunden werden. Microsoft stellt dafür einen Link in der Startleiste zur Verfügung, der den User zur entsprechenden Internetseite weiterleitet.

Alternativ erreicht man diese, wenn man im Internet Explorer auf die Seite <http://v4.windowsupdate.microsoft.com/de/default.asp> geht.

Allerdings wird einem beim Aufruf der Seite, sofern man die vorhin vorgeschlagenen Einstellungen umgesetzt hat, sofort ein Mitteilungsfenster geöffnet, das erklärt, dass die ActiveX-Steuer-elemente nicht ausgeführt werden können. In diesem Fall ist es notwendig, dass man für das Updaten die ActiveX Elemente zumindestens teilweise wieder erlaubt. Da aber das dauernde Umstellen der Einstellungen auf die Dauer lästig wird, ist es vorteilhaft die folgenden 3 Adressen in die Zone „Vertrauenswürdige Sites“ hinzuzufügen:

http://*.windowsupdate.com

http://*.windowsupdate.microsoft.com

https://*windowsupdate.microsoft.com

Außerdem sollte das Windows-Kästchen für die Serverüberprüfung deaktiviert werden.

5.8 Kryptographie

Kryptographie, also die Verschlüsselung von Daten, bietet neue Ansätze im Bereich des Datenschutzes. Aufgrund der zahlreichen kostenlosen Verschlüsselungsprogrammen, die natürlich bei Erwerb einer Lizenz etliche Funktionen mehr haben, ist Kryptographie auch für Privatpersonen interessant geworden. Auf jeden Fall sollte man allerdings nur die kryptographischen Algorithmen verwenden, die in langjährigen Tests von vielen unabhängigen Experten getestet wurden und dadurch ausgereift sind. Es gibt verschiedene Verschlüsselungsverfahren:

- Private-Key-Verfahren
- Public-Key-Verfahren
- Hybride Verschlüsselungstechnik

Ein Private-Key-Verfahren ist ein Verfahren, in dem für die Verschlüsselung und die Entschlüsselung der gleiche Schlüssel benötigt wird. Daher bezeichnet man es auch als ein symmetrisches Verfahren. Ein bekannter in den USA entwickelter Algorithmus ist der DES-Algorithmus. DES steht für **D**ata **E**ncryption **S**tandard. Der Vorteil von Private-Key-Verfahren liegt in der schnellen Verschlüsselung von großen Datenmengen. Doch der sprichwörtliche Haken an diesem Verfahren ist, dass die Sicherheit von der Geheimhaltung des Schlüssels abhängt, der leicht sei es durch Zufall, Nachlässigkeit oder Vorsatz in falsche Hände geraten könnte.

Das Public-Key-Verfahren besteht im Gegensatz zum Private-Key-Verfahren aus 2 Teilschlüsseln. Es wird jeweils der andere Schlüssel für die Entschlüsselung benötigt. Deswegen wird dieses Verfahren auch asymmetrisch genannt. Der erste Teilschlüssel ist der öffentliche Schlüssel, da dieser veröffentlicht wird. Dies kann bedenkenlos gemacht werden, weil man mit Hilfe eines Schlüssels nicht den anderen berechnen kann. Der zweite Schlüssel ist der geheime, der unbedingt geheimgehalten werden muss. Mit diesem Verfahren erreicht man 2 Vorteile. Jede mit dem geheimen Schlüssel verschlüsselte Nachricht enthält eine sog. digitale Signatur, da nur eine Person ihn besitzt. Weiters können Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, nur von der Person, die im Besitz des Geheimschlüssels ist, entschlüsselt werden.

Einziger Nachteil dieses Verfahren ist die sehr rechenintensive Verschlüsselung.

Aus diesem Grund eignet es sich nicht wirklich für größere Datenmengen. Ein sehr bekannter asymmetrischer Algorithmus ist der RSA-Algorithmus³⁶.

Die hybride Verschlüsselungstechnik vereint die Vorteile von den beiden vorigen Verfahren, indem die eigentliche Verschlüsselung symmetrisch erfolgt und die Schlüsselverteilung asymmetrisch.

Zwei sehr bekannte und vielseitige Verschlüsselungsprogramme sind PGP, **P**retty **G**ood **P**rivacy, und PEM, **P**rivacy **E**nhanced **M**ail. Beide Programme verwenden eine Kombination der verschiedenen Verschlüsselungsarten um maximale Sicherheit zu gewährleisten. Für Privatpersonen ist vor allem die Kombination mit einem Emailprogramm interessant.

5.9 Ports sperren

Da ein Computer über viele verschiedene Ports³⁷ angesprochen werden kann, ist es sinnvoll diejenigen zu sperren, die nicht verwendet werden. Jedoch ist es nicht ohne den Einsatz einer Firewall oder eines Routers³⁸ möglich.

Ports können in einem von 3 Zuständen sein:

- Offen
- Geschlossen
- Geblockt/Geschützt

³⁶ Benannt nach seinen Entwicklern: **R**ivest, **S**hamir, **A**dleman

³⁷ Ein Port ist ein Kommunikationskanal, der von einem bestimmten Dienst beansprucht werden kann. Es gibt 2 Gruppen von Ports. Die Ports 0 bis 1023 werden von festgelegten Diensten/Anwendungen benützt, z.B.: Port 80 ist reserviert für HTTP, also Webanfragen. Die Ports 1024 bis 65535 stehen für sonstige Anwendungen zur Verfügung.

³⁸ Die meisten Router besitzen eine built-in Firewall.

Im ersten Zustand ist der Port offen für eine Datenverbindung zwischen 2 Rechnern. Ein etwaiger Angreifer ist sowohl in der Lage festzustellen, dass da ein Computer ist, als auch Angriffe auszuführen.

Wenn ein Port geschlossen ist, dann kann er nicht angegriffen werden. Allerdings weiß ein potenzieller Angreifer, dass unter der ausprobierten IP-Adresse ein Computer existiert. Mit dieser Information kann er andere Ports suchen, die möglicherweise offen sind.

Im Gegensatz zu den vorigen entspricht der letzte dem Idealzustand, weil ein Angreifer weder das eine noch das andere machen kann.

Eine Überprüfung, welche Ports offen sind, stellen einige Softwarefirmen, wie zum Beispiel Symantec unter <http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=ie&venid=sym> , zur Verfügung.

Wie sie bei ihrer jeweiligen Firewall bzw. ihrem Router die Ports sperren können, entnehmen Sie aus den entsprechenden Handbüchern.

5.10 Was tun wenn es brennt?

Sollte es dennoch mal der Fall sein, dass der Verdacht besteht, dass sich ein Virus oder ein Wurm in ihrem Computer eingenistet hat, dann empfiehlt es sich keine unüberlegten, übereilten Maßnahmen, wie Computer augenblicklich herunterzufahren, zu setzen.

Stattdessen sollte man sofort eine etwaige aufgebaute Internetverbindung kappen, um zu vermeiden, dass der Schädling sich auf andere Rechner überträgt bzw. er aus dem Internet zum Beispiel Backdoor-Programme herunterlädt. Außerdem sollte man versuchen den Schädling zu identifizieren und natürlich schleunigst den Virenschanner auf den neuesten Stand zu bringen. Ebenso kann es nicht schaden sich den für den Schädling entsprechenden Remover zu beschaffen.

Da man dem System ab dem Zeitpunkt der Infektion nicht mehr vertrauen kann, sollte man sich die Updates auf einem virenfreien Computer besorgen und dann auf einer Diskette bereitstellen. In weiterer Folge ist es deswegen notwendig den Computer mit Hilfe einer sauberen, also virenfreien, Startdiskette hochzufahren, um jeden in wichtigen Systemdaten eingekisteten Virus auszutricksen. Danach ist es unumgänglich die ganze Festplatte nach befallenen Dateien zu scannen. Da jedoch viele Viren die meisten Antivirenprogramme aushebeln, muss man, um kein Risiko einzugehen, den Scanner neu installieren und mit dem zuvor heruntergeladenen Update „füttern“. Nun sollte es kein Problem darstellen, mit Hilfe des Removers und dem Virenschanner jegliche Spuren des Schädlings zu bereinigen.

Nach der Entfernung des Eindringlings kann es allerdings sein, dass die Programme, deren Programmdateien infiziert waren, neuinstalliert werden müssen. Ebenso könnte es sein, dass die Firewall vom Virus in Mitleidenschaft gezogen wurde und daher eine Reinstallation nötig ist. Jedoch ist es nur in den seltensten Fällen wirklich notwendig das Betriebssystem neu zu installieren.

Zusätzlich sollte man sich vergewissern, ob es nicht neue Updates für das OS gibt, um zum Beispiel eine erneute Infektion zu vermeiden.

Wenn der Verdacht besteht, dass ein Angreifer versucht sich Zugang in das eigene System zu verschaffen, dann sollte auch in diesem Fall die Internetverbindung sofort beendet werden. Anzeichen für solche Angriffe sind neben einer ungewöhnlich hohen Festplattenaktivität auch das massive Schwinden von Festplattenkapazität und eine deutlich spürbare Verlangsamung des Computers.

Im schlimmsten Fall kann wegen des Angriffes ein Neuaufsetzen des Computers inklusive Festplattenformatierung³⁹ notwendig werden, damit der Rechner wieder einwandfrei arbeiten kann.

³⁹ Zuvor sollten alle persönlichen Daten durch ein Backup gesichert werden, da diese durch die Formatierung sonst unwiderruflich verloren wären.

6. Conclusio

Grundsätzlich hinken alle Abwehrmechanismen den Ideen der Angreifer nach. Jedoch hat sich ein Regelkreis entwickelt, der Experten in die Lage versetzt innerhalb weniger Stunden auf Angriffe zu reagieren. Dazu ist es allerdings notwendig die Upgrades regelmäßig einzuspielen. Das optimale Ziel den Computer vor etwaigen Angriffen zu schützen, wird durch Präventivmaßnahmen erreicht, wobei jedem bewusst sein soll, dass es keinen 100% Schutz gibt.

Prinzipiell kann auf 2 Ebenen Schutz betrieben werden:

- durch Hardware, wie Router, Proxy-Server, externe Firewall, etc.
- durch Software, z.B. Antivirens Scanner, Softwarefirewalls, usw.

Schlussendlich sind meiner Meinung nach alle technischen Vorkehrungen empfehlenswert, um maximalen Schutz zu erreichen, allerdings ist der beste Schutz sinnlos, wenn man aus Unachtsamkeit jeden Mailanhang öffnet.

7. Quellenverzeichnis

- [1] Dr. Karlhorst Klotz:
Dr. Klotz' Computerschutz.
Bonn 2003.

- [2] Norbert Pohlmann:
Firewallsysteme – Sicherheit für Internet und Intranet.
Bonn 1998.

- [3] Silvia Barnert, Martin Boeckh, Dr. Matthias Delbrück, u.a. :
Der Brockhaus – Computer und Informationstechnologie.
Mannheim 2003.

- [4] Deborah Russel, G.T. Gangemi Sr. :
Computer Security Basics.
Sebastopol (USA) 1992.

- [5] Heiko Mergard, Christoph Hoffmann, Oliver Ibelshäuser,
u.a. :
Windows sicher machen.
In: PC Professionell Nr. 3 Februar 2004, Seite 36-50.

- [6] Konstantin Breyer:
Skandalöse Sicherheitslücken.
In: PC Professionell Nr. 3 Februar 2004, Seite 118-127.

- [7] Jürgen Schmidt:
Unter fremder Kontrolle.
In: c't Heft 3 2004, Seite 118-121.

- [8] Chaos Computer Club (2003):
Hackerethik.
<http://www.ccc.de/hackerethics>
- [9] Microsoft Security (2003):
Shop Safely Online this Holiday Season.
<http://www.microsoft.com/security/incident/spoof.asp>
- [10] DFN-CERT: Informationsbulletin DIB-2000:01 (2000/2001):
Beschreibung von DoS bzw. DDoS Attacken.
<http://www.cert.dfn.de/infoserv/dib/dib-2000-01.html>
- [11] Thomas Rieske (2003):
Viren und Microsoft Office: Was taugen die Bordmittel?
<http://www.pcwelt.de/ratgeber/viren/31584/>

Autor:

Christian Andreas Feigelbinder

Adresse: Donizettiweg 54/1, 1220 Wien

Klasse 8C

E r k l ä r u n g :

Hiermit erkläre ich, dass ich die vorliegende Fachbereichsarbeit selbst verfasste und nur die angegebenen Quellen verwendete.

Wien, am 14. Februar 2004

Christian Feigelbinder