Inhaltsverzeichnis

Bist du sicher?

Sicherheit? Brauch ich nicht!

Prima! In diesem Fall gehe ich davon aus, dass

- du keine Daten auf deinem Rechner gespeichert hast, die du noch benötigst,
- es dich nicht stört, dass irgendwer deine Mails liest,
- dein Chef, dein Freund oder deine Kinder (die erfahrungsgemäß ohnehin mit den Kisten besser umgehen können als unsere Generation) weiß, wann du auf welche Internetseite gegangen bist,
- jeder in deinem Netzwerk auf all deine Daten zugreifen darf,
- Zugangsdaten öffentlich zugänglich sind,
- du dich nicht daran störst, dass andere jeden deiner Tastaturanschläge mitverfolgen können,
- du kein Problem damit hast, dass andere deine Zugangsdaten für Online-Banking und andere Dienste erfahren,
- du regelmäßig deinen Rechner säubern kannst, weil wieder irgend so ein Programm deine Registry zerschossen hat, sodass du nicht mehr online gehen kannst,
- du gern öfter mal deinen Rechner neu installierst, weil irgendwie gar nichts mehr geht.

und, und, und. Wenn dich all das also nicht stört, dann schlage das Heft zu, es wird dir nicht weiterhelfen.

Poweruser-Know-how

Wenn du andererseits genug Erfahrung gesammelt hast, um zu wissen, dass ich mit den oben genannten Punkten keineswegs übertreibe, dann hast du sicherlich auch Interesse daran, deinen PC möglichst „dicht“ zu machen.

Dieses Heft richtet sich also an Leute, die bereits einige Erfahrung mit Windows gesammelt haben und mehr über die Sicherheitsaspekte wissen wollen.

Du solltest neben den erwähnten Windows-Kenntnissen schon ein wenig Internet-Erfahrung und vor allem Interesse an den Zusammenhängen haben.

Was lerne ich hier?

Wenn du wirklich wissen willst, was läuft, bist du hier genau richtig! Wir werden neben den IT-Sicherheitsgrundlagen und den Windows-eigenen Sicherheitsmechansimen auch topaktuelle Sicherheitslücken aufzeigen. Du wirst lernen, wie diese Angriffe funktionieren und wie du dich effektiv dagegen schützt.

> *IT* steht übrigens für *Informations-Technologie*. Das umfasst alles, was mit EDV zu tun hat, einschließlich der Hardware.

Wir werden an geeigneten Stellen sogar etwas in die Tiefe gehen, um dein Verständnis für die Zusammenhänge zu fördern. Ich stehe auf dem Standpunkt, dass du deinen Feind gut kennen musst, um dich effektiv zu verteidigen.

> Sicherheit ist kein Zustand, sondern ein Prozess! Was heute noch sicher ist, kann morgen schon eine Sicherheitslücke darstellen!

Daher schauen wir sooft es geht hinter die Kulissen – und werden Erstaunliches und auch Erschreckendes entdecken.

Du wirst feststellen, dass es nicht ausreichend ist, mal eben ein Antivirenprogamm und eine Firewall zu installieren und sich dann für alle Zeit zurückzulehnen: „Mein Rechner ist jetzt sicher!“

Ich arbeite bei einem der größten Anbieter für Internet-Sicherheit. Wir betreuen viele große Firmen-Kunden mit teilweise riesigem Sicherheitsaufwand. Und selbst hier gibt es keinen absoluten Schutz.

> Die Angriffsformen werden immer komplexer und raffinierter. Durch die Kombination verschiedener Mechanismen werden häufig neue Angriffe möglich.

Wir werden das Ganze des Öfteren auch mal aus der Sicht des Angreifers betrachten.

Dich erwartet also eine faszinierende Reise in die dunklen Seiten der Cyberwelt. Steig ein und schnall dich an! Es geht rund …

Vor welchen Bedrohungen muss ich mich schützen?

In der Astronomie gibt es einen sehr bezeichnenden Satz:

Alles, was nicht explizit von der Wissenschaft ausgeschlossen wird, existiert irgendwo im Universum!

In der IT-Sicherheit muss man das sogar noch etwas weiter fassen:

> Es gibt nichts, was es nicht gibt!

Mag ein Angriff heute auch noch so undenkbar sein – morgen ist er vielleicht schon Realität. Das hängt sicherlich auch mit der rasanten Entwicklung in der IT-Branche zusammen.

Doch kommen wir wieder zurück in die aktuelle Realität – werfen wir einen Blick auf die wichtigsten Bedrohungen.

Klassisch: Viren, Würmer, Trojaner

An was denkst du als Erstes, wenn du über das Thema IT-Sicherheit nachdenkst? Wahrscheinlich an die klassischen Schädlinge: Viren, Würmer und Trojaner.

Dieses lästige Dauerproblem erscheint in immer neuen Varianten. Inzwischen ist die Artenvielfalt so groß, dass die Hersteller von Antivirus-Software dazu übergehen, Buchstaben paarweise für die Mutationen zu verwenden. Wir werden gleich im nächsten Kapitel hinter die Kulissen dieser automatisierten Hacker schauen. Du wirst die Mechanismen kennen lernen und dich wundern, wie raffiniert diese Biester vorgehen. Irgendwie wie Spinnen: Faszinierend, aber man will sie nicht in seiner Nähe haben …

Java, ActiveX & Co: Aktive Inhalte

Kaum eine Webseite kommt noch ohne Java Script, Java-Applets oder andere aktive Inhalte aus. Schick sieht es ja aus. Und dass der Benutzer mitspielen darf – man nennt das Interaktivität – ist sicher auch eine tolle Sache, da fühlt man sich gleich wichtiger …

Dumm nur, dass das Ganze ein ziemliches Sicherheitsrisiko darstellt: Es gibt zwar verschiedene eingebaute Schutzmechanismen, doch die lassen sich durch Programmfehler oder Fehler im Konzept oftmals aushebeln – ich zeige dir, wie das funktioniert und wie du dich schützen kannst.

Exploits: System-Schwachstellen

Kein Programm ist perfekt. Auch kein Betriebssystem. Es werden immer wieder Programmierfehler gefunden, die durch so genannte *Exploits* ausgenutzt werden können.

> Ein *Exploit* ist ein Stückchen Programmcode oder eine Reihe von Schritten, womit sich eine Sicherheitslücke in einem Programm bzw. einem Betriebssystem ausnutzen lässt.

Ziel dieser Angriffe ist es, auf irgendeine Weise Kontrolle über den angegriffenen Computer zu bekommen – sei es, um sich über Mail weiter zu verbreiten – gern von Würmern genutzt –, ein Programm auf dem Opferrechner zu installieren – z. B. zum Ausspähen von Daten – oder eine so genannte *Backdoor* einzurichten – eine Art Hintertür für einen Angreifer über das Internet.

Meistens entstehen diese Sicherheitslöcher durch einen *Buffer Overflow*. Was das ist und wie es funktioniert, zeige ich dir ebenso, wie die Gegenmaßnahmen, mit denen du dich schützen kannst.

Dialer

Sind heute nicht mehr das beherrschende Thema wie noch vor einigen Jahren – Grund sind der technische Fortschritt (DSL ist wesentlich weiter verbreitet als früher) und die Tatsache, dass es für den Computernutzer einfacher ist, Betrügern die Zahlung zu verweigern. Damit ist es für viele Betrüger uninteressant geworden, sich mit diesem Thema zu beschäftigen.

Spyware

Hierunter fallen alle Programme, die, ohne dich darüber zu unterrichten, Informationen über dich sammeln und diese irgendwem zusenden.

Oftmals werden solche Funktionen in anderen Programmen versteckt, die z. B. als so genannte *Adware* zusätzliche Funktionen für ein bereits installiertes Programm (z. B. Internet Explorer) versprechen.

So kannst du dir mittels Adware eine neue Toolbar für den Explorer einrichten – und nebenbei installierst du damit gleich (ohne es zu wissen, versteht sich) einen *Keylogger*. Das ist ein Programm, das sämtliche gedrückten Tasten mitschneidet. So lassen sich prima Passwörter ausspähen.

Spionage aus dem Internet

… darunter fallen all die Versuche der bösen Jungs, Informationen über dich zu bekommen. Das geht nämlich auch ganz ohne Spyware! Es ist erschreckend, was man über dich herausfinden kann, wenn man nur danach sucht.

Ich zeige dir, was du alles so über dich verrätst, während du im Internet surfst. Natürlich werde ich dir auch wirksame Methoden zeigen, damit deine Akte bei wem auch immer möglichst leer bleibt.

Spam

Keine eigentliche Gefahr, aber *sehr* lästig. Sehen wir uns an, wie wir der nervigen Mailflut Herr werden können.

Social Hacking

Eng verwandt mit Spam ist das „Social Hacking" – der Versuch, per E-Mail an wichtige Daten von dir zu kommen oder dir Trojaner unterzujubeln.

Lokale Angriffe

Im Heimbereich ist ein „Angriff" auf deinen Rechner zwar nicht so wahrscheinlich, aber vielleicht möchtest du trotzdem sicherstellen, dass deine vertraulichen Daten auch vertraulich bleiben. Hierzu bietet Windows einige Möglichkeiten. Darüber hinaus schauen wir uns das eine oder andere Programm an, mit dem du sicherstellen kannst, dass nur der an deine Daten herankommt, der auch die Berechtigung dazu hat.

Außerdem gibt es ja auch noch das Büro und vielleicht den einen oder anderen neugierigen Kollegen oder Chef.

Gegenmaßnahmen

Um gegen all diese Bedrohungen gewappnet zu sein, müsstest du eigentlich in der Zukunft leben. Leider sind uns die bösen Jungs immer einen Schritt voraus – das liegt in der Natur der Sache: Zunächst wird eine Schwachstelle entdeckt, erst dann kann sie geschlossen werden.

Andererseits kannst du durchaus einige Maßnahmen ergreifen, um deinen Rechner „dicht" zu machen, also zu schützen. Aber einen hundertprozentigen Schutz gibt es aus den oben erwähnten Gründen nicht. Die Guten hinken immer einen Schritt nach! Ich hatte es ja schon erwähnt:

> Sicherheit ist ein ständiger Prozess!

Um ein gut abgesichertes System zu haben, musst du u. a.

- die Virensignaturen für dein AV-Programm ständig aktuell halten,
- deine Personal Firewall gut konfigurieren und mittels Penetrationstests erproben,
- dein Betriebssystem und die wichtigsten Anwendungen auf dem aktuellen Patch-Stand halten,
- Programme, die über das Netzwerk kommunizieren, sicher konfigurieren (z. B. den Browser und den E-Mail-Client),
- dich bezüglich neuer Schwachstellen, aber auch neuer Viren, Würmer und Trojaner auf dem neuesten Stand halten und
- dir ein gutes und sicherheitsbewusstes Verhalten aneignen (also z. B. keine vertraulichen Daten wie Bankverbindung, Kennworte etc. auf deinem Rechner speichern).

Hierbei handelt es sich nur um eine Auswahl von Maßnahmen, die für gute PC-Sicherheit notwendig sind.

Wichtig ist vor allem der letzte Punkt; denn du bist einerseits das wichtigste Element in diesem System, andererseits aber das anfälligste …

Nur wenn du dich richtig verhältst, wird dein System ein gutes Maß an Sicherheit aufweisen.

Ich werde dir zeigen, worauf du achten musst, wo Schwachstellen sind und wie du sie beseitigst bzw. schützt.

Da die Bedrohungen manchmal eine Kombination aus verschiedenen Maßnahmen erfordern, bzw. an verschiedenen Stellen auftauchen können, werden wir die Themen im Heft etwas anders gliedern. Du wirst aber für alle oben genannten Angriffe klare Lösungsvorschläge bekommen.

Und wer sind die bösen Jungs?

Echte Hacker, die nur um der Herausforderung willen gezielt in ein Rechnersystem eindringen – oder aber um die Schwachstellen aufzuzeigen – gibt es heute kaum noch.

Stattdessen gibt es so genannte *Skript Kiddies*, die – ohne selbst das notwendige Know-how mitzubringen – fertige Tools benutzen, um entsprechende Schwachstellen auszunutzen. Oft kommt hier noch ein wenig kriminelle Energie oder auch nur einfache Gedankenlosigkeit hinzu. Es geht dann eben

nur noch darum, so viel Schaden wie möglich zu verursachen und damit Aufmerksamkeit zu bekommen. Das Opfer ist dabei völlig egal. Das macht diese Kids so gefährlich.

Bot-Netze

Eine Bedrohung, die in den letzten Jahren immer deutlicher wurde, ist die durch die organisierte Kriminalität. Denn auch das Verbrechen geht mit der Zeit. Kriminelle aus aller Welt versuchen, durch Trojaner so genannte „Bot-Netze" aufzubauen, um dann ferngesteuert Firmenrechner lahmzulegen, Computer von Konzernen oder Regierungen auszuspionieren oder massenhaft Spam zu versenden.

Was sind Bot-Netze?

Das Wort Bot-Netz ist die Kurzform von Roboter-Netz. Es ist ein Verbund von oft mehreren tausend oder sogar hunderttausend Rechnern, die miteinander kommunizieren und ferngesteuert werden. Das geschieht aber nicht etwa freiwillig und mit Wissen der Rechnerbesitzer, sondern durch Einschleusung von so genannten Trojanern. Du könntest im Zweifelsfalle also in ein Bot-Netz integriert sein, ohne die leiseste Ahnung davon zu haben.

Bot-Netze werden beispielweise zum Versenden von Spam verwendet, können im Verbund aber auch wirkungsvolle „Attacken" auf Rechner von Firmen und Organisationen durchführen.

Im Rahmen des zweiten Irak-Krieges versuchten Hacker, Regierungsrechner der USA zu sabotieren – mit mehr oder weniger Erfolg. Auch in der Auseinandersetzung zwischen dem Staat Israel und den Palästinensern gab und gibt es immer wieder solche Versuche.

Mehr zu Bot-Netzen erfährst du ab Seite 60.

Sprechen Sie TCP/IP?

Damit du einen Einblick in die Kommunikation im Internet bekommst, werde ich dir in aller Kürze dein Rüstzeug für das Verständnis von Würmern und Trojanern und deinem besten Freund, der Firewall, darlegen. Das meiste, was ich dir hier zeige, kannst du an späterer Stelle anwenden. Los geht's:

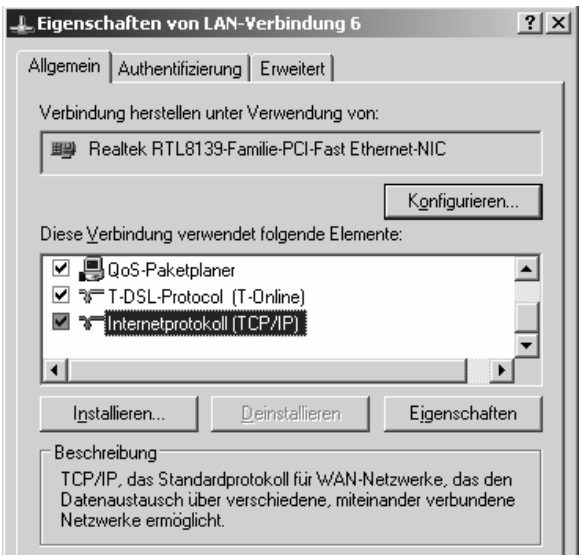
Das im Internet verwendete Kommunikationsprotokoll ist TCP/IP (sprich: Ti Si Pi Ei Pi). Damit wird eine ganze Protokollfamilie bezeichnet, wobei TCP (Transmission Control Protocol) und IP (Internet Protocol) lediglich die Namen gebenden Protokolle sind. Diese Protokolle bauen teilweise aufeinander auf und dienen auf unterschiedlichen Kommunikationsebenen jeweils einem bestimmten Zweck. Fast jede Anwendung im Internet hat ihr eigenes Protokoll, z. B.:

Anwendung	Protokoll
Web (WWW)	HTTP
E-Mail	SMTP, POP3, IMAP
Dateiübertragung	FTP
Namensauflösung	DNS

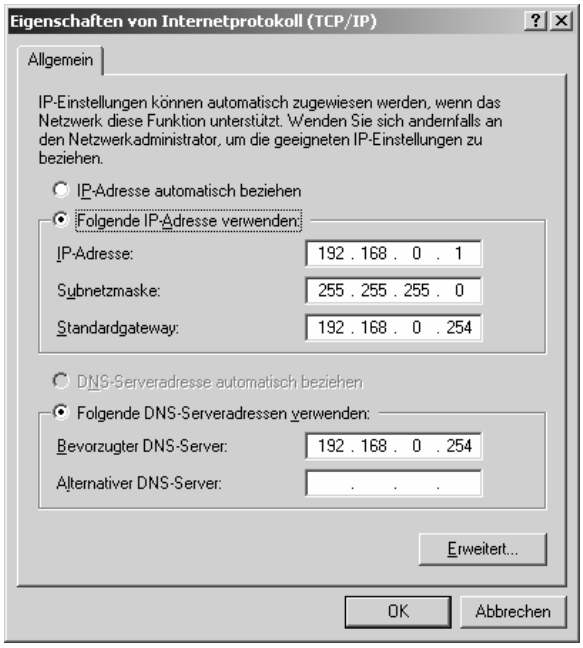
Das sind nur ein paar Beispiele – weitere wirst du kennen lernen.

IP – das Internetprotokoll

Hast du ein Heimnetzwerk oder einen DSL-Zugang? Dann klicke rechts auf deine *Netzwerkumgebung* und lass dir die EIGENSCHAFTEN anzeigen. Hier kannst du dir auch die Eigenschaften deiner Netzwerkkarte ansehen.



Markierst du INTERNETPROTOKOLL (TCP/IP) und klickst auf EIGENSCHAFTEN, bekommst du auch hierfür das Konfigurationsfenster angezeigt:



Wie du siehst, kannst du hier eine *IP-Adresse*, eine *Subnetzmaske*, ein *Standard-Gateway* und einen oder zwei *DNS-Server* angeben. Darauf komme ich gleich zurück. Zunächst ein paar Worte zur untersten Ebene einer Netzwerkkommunikation:

Im lokalen Netz (LAN – Local Area Network) und zwischen deinem PC und dem DSL-Modem oder -Router kommunizierst du über *Ethernet*.

> *Ethernet* ist eine Übertragungstechnik für lokale Netzwerke (z. B. innerhalb eines Gebäudes).

Wenn wir den Datentransport im Netzwerk mit dem Transport von Gütern auf der Straße vergleichen, dann wäre Ethernet die Straße bzw. der Belag; das, auf dem alles basiert.

> In Weitverkehrsnetzen, so genannten WANs (Wide Area Network), kommen andere Übertragungstechniken zur Anwendung, z. B. ISDN oder DSL.

Das wäre dann eben eine andere Art von Straße. Aber die logische Ebene ist dieselbe.

Bauen wir nun das Transportvehikel auf. Zunächst brauchen wir Räder, dazu dient das Internet Protocol (IP). Auf dieser Ebene werden Adressen vergeben, so genannte *IP-Adressen*. Es handelt sich um vier Zahlen zwischen 0 und 255, jeweils durch einen Punkt voneinander getrennt. So könnte bei dir z. B. die IP-Adresse 192.168.1.1 stehen.

Der merkwürdige Zahlenbereich 0–255 beruht darauf, dass jede Zahl einem Byte entspricht. Und ein Byte kann eben genau die oben genannten Zahlen darstellen.

Zu jeder IP-Adresse gehört auch eine Subnetzmaske. Diese teilt die IP-Adresse in einen *Netz-* und einen *Hostanteil* auf. So würde z. B. eine Subnetzmaske von 255.255.255.0 die ersten drei Byte der IP-Adresse dem Netz zuordnen und nur das letzte Byte als Hostanteil deklarieren.

Vereinfacht legt man die Subnetzmaske Byte für Byte (eigentlich Bit für Bit) auf die IP-Adresse. Dort, wo 255 steht, gehört das entsprechende Byte in der IP-Adresse zum Netz. Hier ein Beispiel:

IP	192	168	5	13
SNM	255	255	255	0
Gehört zu	Netz			Host

Während der Netzanteil für alle IP-Adressen gleich bleibt, ändert sich der Hostanteil für jeden Host. Jedes Netzwerkgerät hat also seine eigene IP-Adresse:

192.168.5.1

192.168.5.2

192.168.5.3

usw. bis 192.168.5.254.

> Die letzte Adresse in einem Netz (hier 192.168.5.255) ist für Rundrufe in das lokale Netz reserviert, im Fachjargon auch *Broadcast* genannt.

Das Netz wird übrigens mit Nullen aufgefüllt angezeigt und mit der Subnetzmaske angegeben:

192.168.5.0 255.255.255.0

Achtung – im zweiten und dritten Byte ist ebenfalls eine Null als Teil der Adresse erlaubt. Bei

192.168.0.0 255.255.255.0

ist der Netzanteil trotzdem 192.168.0.

Router – die Pfadfinder

Alle Geräte innerhalb eines logischen Netzwerkes können direkt miteinander kommunizieren. Für die Kommunikation zwischen einzelnen Netzen brauchen wir *Router* oder *Gateways*. Diese Geräte haben je ein Bein in den benachbarten Netzen und vermitteln zwischen ihnen.

Verbindung zwischen Netzwerken – die Router

Möchte also 192.168.5.5 mit 10.0.0.7 kommunizieren, dann wird das über beide Router weitergeleitet. Die durch / getrennten Zahlen bezeichnen übrigens die „gesetzten" Bits in der Subnetzmaske. Pro Byte können 8 Bits gesetzt werden, d.h. den Wert 1 erhalten. Dies beruht auf der binären Rechenweise von Computern, die nur Nullen und Einsen erlaubt (mehr Werte kennt ein Bit auch nicht!).

gesetzte Bits	Subnetzmaske dezimal
8	255.0.0.0
16	255.255.0.0
24	255.255.255.0

Wie du siehst, können die Bits immer nur von links durchgängig gesetzt werden. Zwar gibt es auch andere Netzmasken (z. B. 255.255.224.0), aber die lassen wir hier raus.

Das *Standard-Gateway* ist das Gateway, wohin alle Pakete gesendet werden, die nicht im lokalen Netzwerk liegen und für die es auch keine andere spezielle Route gibt. Das Standardgateway hat immer eine IP-Adresse im gleichen Netz wie der betreffende Computer.

Normale Rechner haben nur einen Weg nach draußen; eben jenes Standardgateway, das du dann auch im Dialogfenster eingeben kannst (und musst, wenn du ins Internet willst).

Für unsere Zwecke gilt: *Gateway=Router*. Die Router im Internet haben z.T. riesige Listen mit IP-Netzwerken, sodass sie wissen, wohin ein Paket zu *routen* ist, damit es auch sein Ziel erreicht.

Um bei unserem Straßenmodell zu bleiben, könnte man die Router als Straßenschilder und Ampeln betrachten, also die Verkehrsregelung.

TCP – Transport der Nutzlast

Bauen wir unser Modell etwas weiter aus. Neben den Rädern brauchen wir auch ein Chassis, bzw. eine Ladefläche für die Waren. Im Netzwerk-Jargon spricht man von *Nutzlast* oder *Payload* (der Begriff *Payload* wird dir gleich noch einmal bei den Viren und Würmern begegnen).

Um diese Nutzlast zu transportieren, bedient sich TCP/IP meistens des Namen gebenden Protokolls *TCP* (Transmission Control Protocol).

An dieser Stelle eine kurze Erklärung zum Aufbau eines „Protokolls“: Das Protokoll enthält zunächst einmal einen *Header*, der die Verwaltungsfunktionen enthält (z. B. Quell-IP-Adresse, Ziel-IP-Adresse, Quell- und Zielport, Checksummen, etc.). Dahinter folgt die jeweilige *Payload* des Protokolls. Da die Protokolle auf unterschiedlichen Ebenen arbeiten, sind sie häufig ineinander verschachtelt. Für IP ist TCP z. B. Teil der Payload.

Ein Datenpaket mit IP und TCP-Header

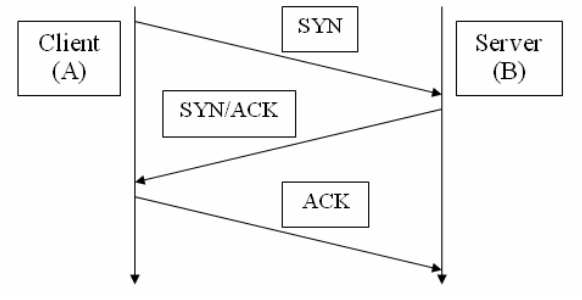
Manchmal hat ein Protokoll auch noch einen *Trailer*, also einen Anhang mit weiteren Verwaltungsinformationen.

Im Endeffekt besteht ein *Datenpaket* also aus den ineinander geschachtelten Protokollen und deren Nutzlast, wobei ein Protokoll auf höherer Ebene zur Nutzlast eines niedrigeren Protokolls gehört.

3-Way-Handshake

Bei TCP handelt es sich um ein verbindungsorientiertes Protokoll ... was heißt das schon wieder?

Nun – es baut eine Sitzung zwischen den Kommunikationspartnern auf, auch *3-Way-Handshake* genannt, weil drei Nachrichten vor Beginn der Sitzung ausgetauscht werden.



Das kannst du dir sozusagen als (formalisierten) Gesprächsbeginn vorstellen. Nehmen wir an, Rechner A möchte mit Rechner B sprechen:

A=>B: *Lass uns reden* (SYN-Flag gesetzt)

B=>A: *okay, bin bereit* (SYN- und ACK gesetzt)

A=>B: *gut, ich fang dann jetzt an* (ACK gesetzt)

Und schon geht die eigentliche Unterhaltung los. Die so genannten *Flags* sind Statusanzeigen innerhalb eines TCP-Headers, um eine entsprechende Reaktion des Zielhosts zu erreichen. SYN steht übrigens für *Synchronisation* und ACK für *Acknowledge* (engl. acknowledge = bestätigen).

Eine TCP-Sitzung wird dadurch beendet, dass einer der Hosts das FIN-Flag setzt (FIN für final, engl. final = Schluss). Der andere antwortet mit FIN und ACK.

Immer noch da? Es stimmt schon – ziemlich harter Tobak. Aber keine Sorge, du wirst später vieles wieder finden!

UDP – Für den Smalltalk

Ein alternatives Protokoll auf derselben Ebene wie TCP ist das *UDP* (User Datagram Protocol). Es wird vorwiegend für den kurzen Nachrichtenaustausch genutzt, z. B. für Namensauflösung (DNS) oder für Statusabfragen (SNMP). Dieses Protokoll baut keine Sitzung auf, es ist *verbindungslos*.

Bis auf bestimmte Ausnahmen nutzen Würmer und Trojaner normalerweise TCP als Transportprotokoll.

Ports – Die Eingangstüren

Auf der Transport-Ebene wird nicht einfach zwischen Rechner A und Rechner B kommuniziert. Damit die verschiedenen Anwendungen ihre Dienste gleichzeitig auf demselben Rechner anbieten können, werden sie an so genannte Ports gebunden.

Es gibt 65535 Ports auf jedem Rechner. Die ersten 1023 sind als *Well known Ports* bekannt und werden auch als *privilegierte Ports* bezeichnet. Es handelt sich um reservierte Ports, auf denen bestimmte Serverdienste ansprechbar sind. Hier eine kurze Auflistung einiger wichtiger Dienste:

Dienst	Port
FTP (File Transfer Protocol, Dateiübertragung)	21/tcp
SSH (sichere Remote-Konsole)	22/tcp
Telnet (unsichere Konsole)	23/tcp
SMTP (Mail-Protokoll)	25/tcp
DNS (Internet-Namensauflösung)	53/udp
HTTP (WWW)	80/tcp
POP 3 (Mail-Abholung)	110/tcp
IMAP 4 (Mail-Abholung)	143/tcp
HTTPS (SSL/TLS, sicheres WWW)	443/tcp

Ports ab 1024 aufwärts werden oft (nicht immer!) vom Client als Absender-Port verwendet. Dies wird vom Betriebssystem gesteuert und kann normalerweise nicht konfiguriert werden.

Du kannst also z. B. folgende Kommunikation verfolgen:

Client: 212.17.3.57 Quell-Port: 1586

Server: 62.16.5.213 Ziel-Port: 80

Damit versucht sich ein beliebiger Client auf einen Webserver auf der entsprechenden IP (man lässt „-Adresse“ häufig weg) auf Port 80, sprich, HTTP bzw. WWW, zu verbinden.

Pro Rechner kann ein Port immer nur von einem Dienst belegt sein. Du kannst also nicht gleichzeitig Mail und WWW über den gleichen Port machen (bei Webmail wird die Mail in http verpackt!). Jeweils ein Dienst bindet sich an einen Port. Zu einem Port gehört dann auch immer die Angabe des Transportprotokolls (TCP oder UDP). Damit bindet z. B. der Webserver den Port 80/tcp. DNS-Server binden normalerweise den Port 53/udp.

Profiwissen: Jeder TCP/IP-Rechner (unabhängig vom Betriebssystem) hat eine Liste bzw. Datei mit Portbelegungen namens *services*. Bei Windows 2000/XP liegt diese unter

```
%systemroot%\system32\drivers\etc.
```

Dabei steht *%systemroot%* als Systemvariable für das Windows-Installationsverzeichnis, meist `c:\windows` oder `c:\winnt`. Schau dir die Liste mal an – es gibt eine ganze Menge standardisierter Dienste. Keine Sorge – nicht alle laufen auf deinem Rechner. Welche Dienste dein Rechner zur Verfügung stellt, werden wir später feststellen.

ICMP – Der Meldegänger

Das *Internet Control Message Protocol* (ICMP) dient dazu, bestimmte Status- oder Problemmeldungen zwischen Rechnern, Routern und anderen Netzwerkgeräten auszutauschen. So wird z. B. auch der *Ping*-Befehl zum Austesten der Verbindung zwischen zwei Rechnern über zwei ICMP-Meldungen realisiert (Typ 8 für *Echo-Request* – die Anfrage, und Typ 0 für *Echo Reply* - die Antwort).

Kennst du den *Ping*-Befehl? Wechsle einfach in die Eingabeaufforderung und gib

```
ping <Ziel-IP-Adresse>
```

ein, also z. B.

```
ping 192.168.5.13
```

Damit kannst du testen, ob du überhaupt Netzwerkkontakt zu einem anderen Rechner hast

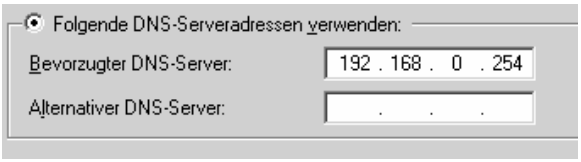
So, jetzt stehen die Anwendungsprotokolle an. Das sind alle Protokolle, die dir einen eigentlichen Nutzen bringen. Die bisher besprochenen Protokolle IP, ICMP, TCP und UDP sind nur Hilfsmittel. Ab jetzt wollen wir Ergebnisse sehen.

Nochmal zur Orientierung: Die Übertragungstechnik (Ethernet, ISDN, DSL) ist die Straße, auf der sich die Räder (IP) bewegen. Diese tragen ein Chassis mit Ladefläche (TCP oder UDP). Die Anwendungsprotokolle sind die Container auf dieser Ladefläche, die die eigentlichen Daten enthalten. Wie im wirklichen Leben interessierst du dich als Anwender eigentlich nur für diese Nutzlast. Und die schauen wir uns jetzt an:

Domain Name Service (DNS)

Weil wir uns viel besser Namen als Zahlen merken können, hat man sich irgendwann einen Namensauflösungsdienst namens DNS ausgedacht. Hast du dich schon mal gefragt, was aus deiner Eingabe: „www.irgendwas.de“ im Browser wird? Kurz gesagt wird sie in eine IP-Adresse umgewandelt, weil das Internet mit der Anfrage nichts anfangen kann. Stattdessen wird eine IP-Adresse benötigt, die du von einem DNS-Server erhältst.

Daher musst du auch mindestens einen solchen Server für deinen PC konfigurieren, damit dieser weiß, wen er für solche „kryptischen“ Anfragen wie z. B. „www.microsoft.de“ fragen soll. Das Ergebnis ist so etwas wie 212.184.80.190. Erst auf diese Antwort hin kann sich dein Rechner mit dem entsprechenden Server verbinden.



Hier gibst du deinen DNS-Server ein

Die Datei „hosts“

DNS arbeitet auf Port 53/udp. Gefährdet bist du dann, wenn eine Anfrage umgeleitet wird und eine falsche Antwort zurückliefert. Das ist zwar aus der Ferne nicht ganz leicht, aber es geht. Eine Methode funktioniert über einen der zahllosen Dinosaurier in den Microsoft-Programmen, die Datei „hosts“, die eine Liste mit Namen-IP-Adressen-Zuordnungen enthält.

Diese Datei liegt bei Windows XP im Verzeichnis `Windows/system32/drivers/etc`. und kann um beliebige Einträge erweitert werden. Man kann dies nutzen, um z. B. Shortcuts zu oft besuchten Webseiten zu definieren – allerdings können manche Programme diese Datei ebenfalls benutzen. Da diese Datei normalerweise zuerst gefragt wird, bevor ein DNS-Server im Internet bemüht wird, kann ein Falscheintrag an dieser Stelle zu einer fehlerhaften Namensauflösung führen.

Aushebelung von Virenschutz-Updates

Manche Würmer nutzen das aus, indem sie die Update-Adressen für verschiedene Virenschutzprogramme und andere auf einen falschen Wert setzen – normalerweise auf die eigene interne Adresse, die bei allen Rechnern 127.0.0.1 ist, diese heißt *Loopback-Adresse*. Damit können sich die Programme nicht mehr mit dem Update-Server verbinden, um z. B. aktuelle Signaturen oder Patches herunterzuladen.

> Ein einfacher, aber zumeist wirkungsvoller Schutz besteht darin, diese Datei mit einem Schreibschutz zu versehen.

WWW – World Wide Web

Unter diesem Teil des Internets verstehen wir die bunten Bilderchen. Diese werden von Webservern über ein Protokoll namens *HTTP* (Hypertext Transfer Protocol) geliefert. Webserver lauschen normalerweise auf Port 80/tcp. Wenn du eine Adresse im Browser angibst, dann verbindet er sich mit der aufgelösten IP automatisch auf Port 80.

Abhörsicher auf Port 443/tcp

Wenn du dich z. B. mit deiner Bank verbindest, oder bei einem Online-Shop eine Bestellung aufgeben möchtest, wird normalerweise abhörsicher kommuniziert. Das geschieht über *SSL* (Secure Socket Layer). Dieses Protokoll arbeitet auf Port 443/tcp. Einzelheiten hierzu reiche ich später im Kapitel über Kryptographie auf Seite 59 nach.

Mail – immer noch am häufigsten

Mail ist nach wie vor die meist verbreitete Internetanwendung. Die Kommunikation geschieht über ein Protokoll namens *SMTP* (Simple Mail Transfer Protocol) über Port 25/tcp.

Nur wenn du Mails von deinem Mailserver abholen willst, kommen andere Protokolle zur Anwendung, nämlich POP3 (Post Office Protocol) auf Port 110/tcp – oder alternativ dazu IMAP 4 (Internet Message Application Protocol) auf Port 143/tcp.

Dein Mailclient – meistens *Outlook (Express)* oder Windows Mail, doch immer öfter auch *Thunderbird* oder andere alternative Mailprogramme – kennt diese Ports und nutzt sie auch für den entsprechenden Zweck.

FTP – Dateitransfer

Das File Transfer Protocol (FTP) wird häufig zum Transportieren von Dateien verwendet. Es arbeitet auf Port 21/tcp für den Verbindungsaufbau und die Verwaltungsinformationen und auf Port 20/tcp für die eigentliche Datenübertragung.

Wenn du FTP verwenden möchtest, schreibst du in der Adressleiste deines Browsers `ftp://` statt

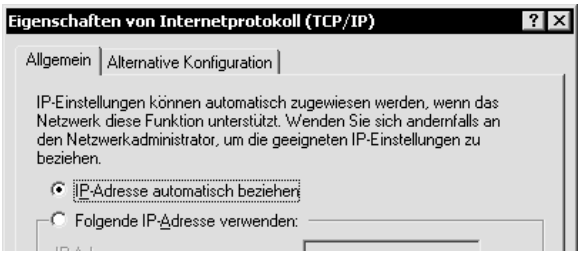
`http://` vorweg. Normalerweise macht das dein Browser aber von allein, wenn du einen Hyperlink anklickst, der auf einen FTP-Server verweist.

FTP hat einen kleinen Bruder, das TFTP (Trivial FTP). Es arbeitet auf Port 69/udp und dient heutzutage vor allem Würmern, um sich zu verbreiten.

DHCP – Gib mir eine Adresse …

Wenn sich ein Computer im Netzwerk anmeldet, kannst du ihm eine dynamische IP-Adresse zuweisen. Das passiert z. B., wenn du dich bei deinem Internet-Provider anmeldest. Der Service hierfür heißt Dynamic Host Configuration Protocol (DHCP) und arbeitet auf Port 68/udp.

Du kannst deinen PC in den Eigenschaften von TCP/IP als DHCP-Client konfigurieren:



Wenn dein Rechner als DHCP-Client eingerichtet ist, dann ruft er beim Start ins Netz hinein und fragt nach einem DHCP-Server. Dieser gibt ihm dann für eine bestimmte Zeitspanne (die so genannte *Lease*-Dauer) eine Konfiguration, mit der er im Netzwerk kommunizieren kann. Danach gibt er die Netzwerkkonfiguration (*Lease* genannt) wieder ab, damit sie für andere Hosts zur Verfügung steht, oder versucht, seine *Lease* zu erneuern.

Hast du einen ISDN- oder DSL-Router, dann kannst du diesen i.d.R. auch als DHCP-Server einsetzen. Dazu definierst du einen bestimmten Adressbereich (z. B. 192.168.0.100 – 192.168.0.150), der dynamisch vom Router vergeben wird.

NetBIOS – wenn Windows spricht

Wie du weißt, kann Windows über Netzwerklaufwerke bzw. Freigaben auf andere Windows-Rechner zugreifen. Ebenso kannst du so einen Netzwerkdrucker ansprechen. Die traditionellen NetBIOS-Ports sind

- 137/udp (Namensdienst),
- 138/udp (Datagrammdienst) und
- 139/udp (Sitzungsdienst).

Auf NetBIOS setzt SMB (Server Message Block) auf, das für die Datenübertragung zuständig ist. SMB nutzt

- 139/tcp (bei älteren Windows-Systemen und
- 445/tcp (ab Windows 2000)

Es ist keine gute Idee, diese Ports für das Internet zu öffnen, da dann jedermann auf deine Freigaben zugreifen kann!

Interessanterweise DARF er das sogar: Der Paragraf 202a StGB (Ausspähen von Daten) besagt, dass nur dann Strafe droht, wenn der Angreifer Daten ausspäht, die gegen unbefugten Zugriff besonders geschützt sind (z. B. per Passwort, etc.). Wenn du dagegen eine normale Freigabe einrichtest, kann in der Voreinstellung jeder darauf zugreifen …

Jetzt aber Pause! Es gibt noch unglaublich viel mehr Protokolle auf der Anwendungsschicht. Wie bereits erwähnt, hat fast jede Anwendung im Internet ihr eigenes Protokoll. Wichtig ist aber diese erste Einführung in die Kommunikationsstruktur des Internets. Mit diesem Wissen gerüstet, können wir uns dem ersten eigentlichen Sicherheits-Thema zuwenden.

Viren, Würmer und Trojaner

In unserem ersten Kapitel über Sicherheit werden wir uns mit nervigen kleinen Programmen mit den obigen Bezeichnungen beschäftigen, die sich ungefragt bei dir einnisten und auf deinem Rechner alles Mögliche anstellen – du wirst staunen, was Viren, Würmer und Trojaner so alles können. Im Grunde genommen setzt nur die Kreativität des Programmierers eine Grenze.

Aber was ist eigentlich der Unterschied zwischen Viren, Würmern und Trojanern? Jeder benutzt diese Begriffe – kannst du mir aber erklären, worin sich ein Wurm von einem Virus unterscheidet? Nein? – Keine Bange – spätestens nach diesem Kapitel kannst du das. ☺

Viren

Ein Computervirus heißt Virus, weil es einige Gemeinsamkeiten mit seinem biologischen Namensvetter hat:

1. Es reproduziert, also verbreitet, sich selbst,
2. Es benötigt einen Wirt, um sich einzunisten. In der Biologie ist das der Mensch – in der Computerwelt ist es eine Datei, an die es sich anhängt, sowie ein Computer, auf dem die Datei ausgeführt wird.

Neben dieser „Verbreitungs"-Funktion enthält jedes Computer-Virus eine Nutzlast, auch Schadensroutine oder *Payload* genannt. Sie enthält Programmcode, der die eigentliche Auswirkung des Virus ausmacht. Die Aktivitäten sind vielfältig und reichen von einfachen Scherzen (z. B. das Geräusch von Wasserblubbern und eine Meldung: „Wassereinbruch in Laufwerk A") bis hin zur totalen Zerstörung aller Daten auf der Festplatte …

Häufig wird die Definition auch weiter gefasst: *Viren sind Programme, die sich selbständig weiterverbreiten*. Diese Definition umfasst auch die Würmer. Diese Untiere werden zwar meist, wie auch hier, separat behandelt, sie werden aber oft schlicht (und genau genommen fälschlicherweise) ebenfalls als Viren bezeichnet.

Virentypen

Es gibt eine fast unüberschaubare Anzahl von verschiedenen Viren – ihre Zahl geht (wenn man die Würmer mitrechnet) in die zehntausende (ca. 70.000). Allerdings sind die meisten davon nur Labor- oder Zoo-Viren – Testviren aus den Antivirenlabors, mit deren Hilfe man mögliche Schädlinge untersucht.

Was gefährlich ist, sind die Viren „In-The-Wild", also auf freier Wildbahn. Es handelt sich um einen Bruchteil der oben genannten Viren – dummerweise sind sie aber im Internet weit verbreitet und für deinen Computer sehr gefährlich.

Wir kennen dutzende verschiedener Kategorien – einige davon möchte ich hier vorstellen:

Bootsektor-Viren

… sind (glücklicherweise) eine fast ausgestorbene Art. Grundsätzlich können Bootsektor-Viren jeden Bootsektor eines Festspeichers befallen.

> Das bevorzugte Übertragungsmedium von Bootsektor-Viren sind Disketten.

Das Virus infiziert den Bootsektor der Diskette und wartet, bis dieser aufgerufen wird. Das passiert, wenn die Diskette eingelegt und z. B. im DOS-Fenster oder im Explorer aufgerufen wird. Das Virus kopiert sich auf die Festplatte und nistet sich danach im MBR (Master Boot Record) der Festplatte oder einem Bootsektor einer Partition ein. Ab dem Neustart des Rechners ist es aktiv.

> Der MBR entspricht den ersten 512 Byte auf einer Festplatte und initialisiert den Start des Betriebssystems.

Bootsektorviren sind die ältesten bekannten Viren. Heute sind sie fast ausgestorben, da Disketten kaum noch verwendet werden.

Die meisten Bootsektorviren sind einfach nur da. Sie haben anscheinend keine Schadenswirkung sondern sind nur an ihrer Verbreitung interessiert, so ähnlich wie viele Würmer.

Es gibt aber auch sehr schädliche Varianten, z. B. *AntiCMOS*, der die Konfigurationsinformationen des CMOS löscht, also des Speicherbausteins, auf dem das BIOS gespeichert ist. Anschließend ist das BIOS nicht mehr zu gebrauchen. Und es kostet Zeit und Geld, ein neues BIOS einzurichten.

So entfernst du Bootsektor-Viren

Das Ärgerliche an diesen Biestern ist, dass sie arbeiten, bevor überhaupt ein Antivirenprogramm geladen wurde – sie sind ja vom Start des Rechners an aktiv.

Bei Windows-Versionen bis Windows 98/ME kannst du mit

```
fdisk.exe /mbr
```

auf der Konsole den alten (nicht infizierten) Bootsektor wieder herstellen.

Wenn du Windows 2000 oder XP hast, hilft dir die *Wiederherstellungskonsole*. Die musst du allerdings erst von der Windows-CD nachinstallieren. Nehmen wir an, dein CD-Laufwerk hat den Laufwerksbuchstaben D – dann gibst du

```
d:\i386\winnt32.exe /cmdcons
```

ein (z. B. über *Start/Ausführen*). Nach der Installation ist die *Wiederherstellungskonsole* über F8 beim Systemstart über das Startmenü zu erreichen.

Damit kannst du dann `fixmbr` aufrufen.

Sollte das Virus einen Start des Systems verhindern, kannst du immer noch über die Windows-CD booten. Dabei wird das *Setup* gestartet. Auch hier kannst du die *Wiederherstellungskonsole* auswählen.

In jedem Fall solltest du danach im *abgesicherten Modus* (auch über F8 beim Start erreichbar) ein Antivirenprogramm durchlaufen lassen, um auch die Reste (evtl. selbst angelegte Kopien des Virus usw.) zu entfernen.

Makroviren

Es ist schon ein paar Jahre her, da waren Makroviren die größte Plage der Computerwelt.

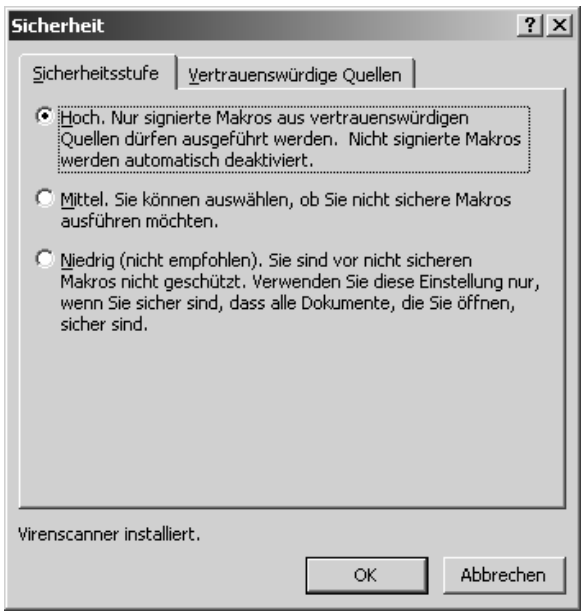
Das Problem ist, dass Microsoft Office mit VBA eine leistungsfähige Programmiersprache zum Modifizieren und Erweitern der Funktionen der Office-Programme mitliefert – dumm nur, dass man damit jeden denkbaren Befehl zur Ausführung bringen kann. Sicherheitsmechanismen gab es praktisch nicht.

Und so konnten sich die Makroviren, die zum größten Teil Word-Makros waren, beliebig verbreiten.

Sinngemäß sah das so aus:

1. Der Benutzer öffnet ein Dokument,
2. in dem Word ein Makro findet und es ausführt;
3. das Virus erwacht und infiziert zunächst alle weiteren Word-Dateien, die es finden kann – u.U. hat es auch noch einen zusätzlichen Verbreitungsweg über andere Dateitypen –
4. und hat es dann seine Vervielfältigung gesichert, führt es seine jeweilige Schadensroutine aus – so kann ein solches Virus z. B. Daten auf der Festplatte zerstören oder verhindern, dass Word gestartet werden kann.

Heute ist das Thema Makroviren so gut wie vom Tisch – ab *Office 2000* wurden eigene Sicherheitsmechanismen eingebaut. Die entsprechenden Einstellungen kannst du in Word unter EXTRAS | MAKRO | SICHERHEIT vornehmen:



Normalerweise reicht die mittlere Option aus – nur bei wirklich sicherheitsrelevanten Daten auf dem Rechner sollte die höchste Stufe gewählt werden.

Leider ist das auch keine perfekte Lösung, da immer wieder neue Sicherheitslücken bekannt werden. Diese können und sollten aber mittels Patch behoben werden. Gib einfach auf der Microsoft-Seite (www.microsoft.de) „Office“ und „Sicherheitsupdate“ und/oder „Servicepack“ als Suchbegriff ein.

Leider kann ich dir keine direkten Download-Links oder URLs geben, weil Microsoft ständig wechselnde Strukturen auf der Website hat und sich die *Locations* also immer wieder ändern. Im Zweifel sind die Links „Downloadcenter" und „Sicherheit" immer heiße Kandidaten auf Erfolg ;-).

Im Übrigen werden Makroviren inzwischen sehr zuverlässig von Virenscannern entdeckt. Wie du auf dem Bild oben erkennen kannst, hat Word erkannt, dass ein Virenscanner (bei mir z. Z. *Norton Antivirus*) installiert ist. Word kann diesen Virenscanner selbständig aufrufen, damit er zu ladende Dokumente überprüft.

Stealth-Viren

Eine der faszinierendsten Unterarten von Viren sind die *Stealth-Viren* (stealth=verdeckt, heimlich). Diese Viren verstehen es, unentdeckt zu bleiben, indem sie bestimmte Tarnmechanismen verwenden.

Während alle Viren naturgemäß zunächst vor dem Anwender versteckt sind (sie sind ja unerkannter Teil eines anderen Programms), schützen sich Tarnkappen-Viren zusätzlich sogar vor der Entdeckung durch Virenschutzprogramme! Das geht z. B. folgendermaßen:

1. Ein Virenscanner will eine Datei öffnen, um sie zu überprüfen.
2. Das Stealth-Virus bemerkt dies, fängt den Aufruf ab und liefert die zuvor gesicherte Originaldatei an den Virenscanner.
3. Der Virenscanner entdeckt natürlich keine Infektion und schließt die Datei wieder
4. Das Virus aktiviert wieder die infizierte Datei.

Soll das funktionieren, muss der „Tarnkappenbomber" speicherresident sein, also permanent im Hauptspeicher des Systems verbleiben. Kein Problem für das schlaue Stück!

Eine andere Methode besteht darin, die von Virenscannern erzeugten Prüfsummen zu löschen. Das Programm muss dann neue erzeugen, die anschließend den Virencode integriert haben … dumm gelaufen.

Polymorphe Viren

… sind Gestalt verändernde Viren und eigentlich eine Unterart der *Stealth-Viren*. Auch sie versuchen unerkannt zu bleiben – und zwar indem sie in unterschiedlichen Formen in Erscheinung treten. Häufig wird der größte Teil des Viren-Codes auf verschiedene Weisen verschlüsselt. Der unverschlüsselte erste Teil enthält die Entschlüsselungs-Informationen. Wird die infizierte Datei aufgerufen, wird der Code zunächst entschlüsselt und dann ausgeführt.

Da die meisten Virenscanner hauptsächlich nach festen Virencode-Signaturen scannen, werden solche Viren auf diesem Wege natürlich nicht entdeckt. Es gibt jedoch Methoden, auch diese Art Viren anhand von anderen Merkmalen zu entdecken, z. B. der Signatur des unverschlüsselten Teils. Die polymorphen Viren haben sich letztlich als nicht so dramatisch erwiesen, wie das zunächst zu vermuten war. Heute werden fast alle polymorphen Viren von Virenschutzprogrammen zuverlässig erkannt.

VBS-Viren

Diese Art Viren sind in der Skriptsprache Visual Basic Script (VBS) geschrieben. Wie bei Microsoft üblich, gab es anfangs natürlich fast überhaupt keine Sicherheitsmechanismen für diese Skriptsprache. Somit konnte sich z. B. *Loveletter*, eigentlich ein Wurm, im Mai 2000 perfekt verbreiten und jede Menge Dinge anstellen.

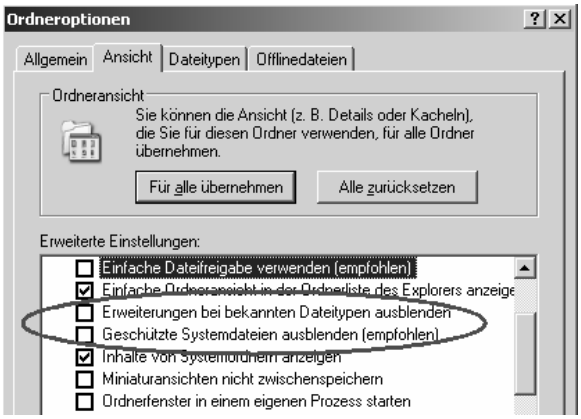
Neben der (fast obligatorischen) Manipulation der Registry, um beim nächstfolgenden Systemstart wieder gestartet zu werden, und dem Erstellen von verschiedenen Dateien wurde auch ein Trojaner aus dem Netz heruntergeladen, um eine Hintertür zu öffnen. Wie du siehst, lässt VBS keine Virenautoren-Wünsche offen …

Übrigens – was ein Trojaner ist, erfährst du ab Seite 27.

Das Gemeine ist, dass VBS-Viren und –Würmer eine Doppelendung haben, z. B. `Bild.jpg.vbs`.

Standardmäßig werden bekannte Endungen von Windows nicht angezeigt, du bekommst also nur noch `Bild.jpg` zu sehen. Da JPG-Bilder keine Gefahr darstellen, klickst du doppelt auf das vermeintliche Bild – und schon wird das VB-Skript aktiv …

Um dieser Falle zu entgehen, solltest du im Windows-Explorer unter EXTRAS|ORDNEROPTIONEN|ANSICHT sofort die beiden markierten Optionen deaktivieren:



Die Option ERWEITERUNGEN BEI BEKANNTEN DATEITYPEN AUSBLENDEN musst du unbedingt abschalten, wenn du doppelte Dateiendungen erkennen willst.

Im Übrigen werden VBS-Viren fast ausschließlich per Mail versandt und benötigen deine Mithilfe, um aktiv zu werden: Du musst die angehängte Datei nämlich mit einem Doppelklick aktivieren … selber Schuld, wenn du es tust!!!

Hybridviren

Klasse Sache, so ein Hybridvirus … für einen Virenautor! Irgendwie sind Hybridviren eine logische Konsequenz aus den bisherigen Viren: Warum sich auf einen Ansatz beschränken, wenn man mehrere Techniken miteinander verbinden kann.

> Die meisten heutigen Schädlinge sind *Hybrid-Viren* bzw. *–Würmer*!

Später sehen wir uns einige zurzeit aktive Schädlinge an. Du wirst feststellen, dass der Übergang zwischen Viren, Würmern und Trojanern inzwischen sehr fließend geworden ist.

Sehen wir uns einfach mal die Schadensroutine des Wurms *Korgo.F* an, der zwar nicht mehr sonderlich aktuell ist, aber immer noch sehr gut das bisher Geschriebene verdeutlicht:

- Er nutzt eine Sicherheitslücke im lokalen Authentifizierungssystem von Windows 2000 und XP (LSASS), um sich über Port 445 (SMB) auf das System zu laden.
- Dann überwacht er die Ports 113 und 3067 auf Kontaktaufnahme und sendet im Falle eines Verbindungsaufbaus eine Kopie von sich selbst an den Client.
- Anschließend verwischt er seine Spuren, indem er bestimmte Dateien löscht und bestimmte Werte aus der Registry entfernt – somit werden verschiedene Update- und Sicherheitsmechanismen des Betriebssystems ausgehebelt.
- Als wäre das nicht genug, versucht er, die LSASS-Sicherheitslücke gegen beliebige IP-Adressen anzuwenden, um sich auf diesem Weg weiterzuverbreiten, und
- eine Funktion in den *Explorer.exe*-Prozess einzubauen, die vorgibt, dass alle Aktivitäten nicht mehr von ihm, als eigenständigem Prozess, sondern von Explorer.exe kommen, und so seine Existenz verschleiert.
- Schließlich versucht er, mit verschiedenen IRC-Servern (das sind Chat-Server) auf Port 6667 Verbindung aufzunehmen, um von dort Befehle zu erhalten.

Wie du siehst, sind solche Biester inzwischen ganz schön clever und haben fast immer mehrere Ansätze, um wirksam zu werden. Für Details kannst du z. B. auf die Symantec-Seite www.symantec.de gehen und *Korgo.F* als Suchbegriff eingeben.

Top-Ten-Liste der Viren

Unter dieser Adresse findest du auch eine Übersicht über die Top-10 der im Umlauf befindlichen Schädlinge: