Einstellungen in Windows, Browser und Mailprogramm

Beitrag von MobyDuck

In dem Beitrag „Bestandsaufnahme“ haben wir gesehen, dass es Schädlinge gibt, die sich ohne Zutun des Users automatisch ausführen und verbreiten. Sie nutzen hierzu Sicherheitslücken in verbreiteten Programmen, insbesondere in Windows, dem Internet Explorer und in Mail-Programmen. Die Sicherheitslücken wiederum können Fehler in den Programmen sein, gerne werden jedoch auch sicherheitskritische Programmfeatures ausgenutzt.

Um sich gegen diese Schädlinge abzusichern, sollte man zunächst das Angebot der Software-Hersteller annehmen und regelmäßig die aktuellen Patches aufzuspielen. Hierauf kommen wir beim Thema „Sicherheitskonzepte“ zurück.

Weiter ist es nötig, die besonders gefährdeten Programme wie Windows und den Internet Explorer so einzustellen, dass sie den Schädlingen eine möglichst geringe Angriffsfläche bieten.

Windows

Eingeschränkte Rechte

Win XP bietet die Möglichkeit, das Dateisystem NTFS zu benutzen. Dieses Angebot sollten wir annehmen, da die Vorteile den Nachteil, etwas langsamer als das Dateisystem FAT zu sein, bei weitem aufwiegen. So haben wir unter NTFS die Möglichkeit, über

Systemsteuerung -> Benutzerkonten

Konten mit eingeschränkten Rechten einzurichten. Es ist zu empfehlen, nur mit diesen eingeschränkten Konten zu surfen, da – vereinfacht gesagt – die meisten Schädlinge zu ihrer Ausführung Administratorenrechte benötigen. Mit eingeschränkten Rechten ist jedoch der Zugriff auf wesentliche Teile der Registry und der Systemdateien nicht möglich (das gilt natürlich auch für Malware, die man anklicken muss).

Wer will, kann dies gleich einmal an einem Beispiel ausprobieren: Wir hangeln uns mit eingeschränkten Rechten im Explorer zu der Datei Windows\System32\drivers\etc\hosts durch und öffnen die Datei mit dem Editor. Jetzt schreiben wir irgendetwas am Ende des Textes hinein und versuchen, abzuspeichern. Der Versuch scheitert mit einer Fehlermeldung. Ebenso würde es einem Hijacker-Script bei dem Vorhaben ergehen, die Datei Hosts zu manipulieren, um auf ungewollte Seiten umzulenken.

Leider hat Microsoft die Rechteverwaltung nicht so konsequent umgesetzt wie z.B. Linux. Das Windows-Update funktioniert nur mit Administratoren-Rechten und auch verschiedene Programme laufen mit eingeschränkten Rechten nicht. Ich halte es daher für einen guten Kompromiss, zumindest konsequent mit eingeschränkten Rechten zu surfen.

XP Professional bietet noch weitergehende Möglichkeiten der Rechteverwaltung, die mit Tools auch für XP Home freigeschaltet werden können. Die richtige Konfiguration ist jedoch reichlich kompliziert. Für die hier interessierenden Zwecke (Abwehr von Schädlingen) reicht die soeben vorgestellte Variante aus.

Unbenötigte Dienste abschalten

XP startet ungefragt eine Vielzahl von sogenannten Diensten, das sind bestimmte Programme, die im Hintergrund ablaufen und teilweise sogenannte Ports ins Internet öffnen. Ich halte es für sinnvoll, unbenötigte Dienste abzuschalten. Hierzu kann man sich des Scripts auf der Seite

http://www.ntsvcfg.de/

bedienen oder noch bequemer das Programm auf der Seite

http://www.dingens.org

benutzen. Auf alle Fälle sollte man auch die Erläuterungen auf beiden (!) Seiten lesen. Wer es sich zutraut, kann natürlich auch manuell unbenötigte Dienste deaktivieren. Listen der unnötigen Dienste finden sich per Google. Gut finde ich diese Aufstellung:

http://www.windows-tweaks.info/html/dienste.html

Das vorstehende gilt sinngemäß für alle NT-Systeme. Nutzer älterer Win-Versionen haben die Möglichkeit der Rechteverwaltung nicht, aber das folgende geht alle an:

Der Windows Scripting Host

Wer den Scripting Host nicht unbedingt benötigt, sollte den WSH abschalten. Im Zusammenspiel mit dem Internet Explorer bietet er nämlich fast unbeschränkte Möglichkeiten, auf ein System zuzugreifen, z.B.:

```
<HTML>
<SCRIPT LANGUAGE="VBSCRIPT">
Set WShell = CreateObject("wscript.Shell")
key="HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\1201"
WShell.RegWrite key, 0, "REG_DWORD"
- hier mache ich natürlich nicht weiter ;-)
</SCRIPT>
</HTML>
```

Wenige Zeilen VB-Script und bis einschl. XP SP1 ist das Zonenmodell des Internet Explorers ausgehebelt. Es können dann z.B. ActiveX-Komponenten ohne Rückfrage gestartet werden.

Unter Win98 lässt sich der WSH noch mit

System -> Software -> Windows Setup -> Zubehör

abschalten. Unter anderen Win-Versionen geht das nicht mehr. Man kann sich damit behelfen, dass man im Explorer die Ordneroptionen öffnet und unter „Dateitypen“: „Registrierte Dateitypen“ die Registrierung für *.vbs-Dateien löscht.

Datei Hosts

Falls man nicht konsequent mit eingeschränkten Rechten surft oder dies nicht kann (bis einschl. Win ME), dann sollte man noch die Datei Hosts mit einem Schreibschutz versehen. Den Pfad unter XP habe ich oben erwähnt, in Win 98 findet sich die Datei unter Windows\Hosts. Einfach die Datei im Explorer mit rechts anklicken, das Attribut „schreibgeschützt“ vergeben und die bei Hijackern beliebte Masche, diese Datei zu manipulieren ist zumindest etwas erschwert.

Browser

Browser sind eigentlich sicherheitsmäßig ziemlich harmlos. Zumeist geht die Gefahr von Zusatzprogrammen aus, die in die Browser eingebaut sind, um das Surfen interessanter und einfacher zu machen. Schauen wir uns diese Programme einmal näher an:

Es gibt zunächst *ActiveX*, eine Softwarekomponente, die z.B. die Einbettung beliebiger Objekte in Webseiten ermöglicht und außerdem zum Informationsaustausch zwischen dem Computer des Users und einem Server genutzt werden kann. ActiveX läuft unmittelbar auf dem System des Users ab und erlaubt einen vollständigen Zugriff auf das System. Dementsprechend gibt es auch nichts, was man sich nicht mittels ActiveX einfangen könnte. Nur der Internet Explorer unterstützt dieses Feature und es sollte unbedingt abgeschaltet werden. Unseligerweise benötigt das XP-Update nicht nur Administratoren-Rechte, sondern auch ActiveX. Man kann sich damit behelfen, dass man die Microsoft-Update-Seiten in die Zone „vertrauenswürdige Seiten“ aufnimmt. Wie das funktioniert, erfährt man von Microsoft, wenn man versucht, ohne ActiveX ein Update zu starten.

Java ist eine plattformunabhängige Programmiersprache. Im Internet wird *Java* vor allem benutzt, um sogenannte Java-Applets, d.h. kleine Zusatzprogramme, zu starten. j-a-v-a ist nicht so unsicher wie ActiveX, da kein Zugriff auf das System erfolgt. Allerdings sind in der Vergangenheit Programmfehler publik geworden, die ein Sicherheitsrisiko darstellten. Diese Fehler sind inzwischen zwar behoben, man weiß jedoch nicht was kommt und sollte daher *Java* – wenn überhaupt – nur auf vertrauenswürdigen Seiten einsetzen.

JavaScript hat mit *Java* nichts zu tun. Es handelt sich um eine Programmiersprache, mit der man z.B. solche Nettigkeiten wie ungefragt aufpoppende Fenster erzeugen kann. Der Einsatz kann jedoch auch nützlich sein, z.B. bei der Eingabe von Formular-Daten etc. Problematisch ist vor allem, dass theoretisch bei aktiviertem j-a-v-a ein

ungewollter Zugriff auf Java-Applets möglich ist. Dies kann man dadurch umgehen, dass man j-a-v-a deaktiviert. Weiter kam *JavaScript* ins Gerede, weil es zur Täuschung des Users missbraucht werden kann. Die Täuschung kann darin bestehen, dem User vertrauenswürdige Seiten vorzuspiegeln, um sensible Daten abzufangen (Phishing) oder das Ziel eines Links zu vertuschen.

Die Microsoft-Variante heißt *JScript*. Diese Version von *JavaScript* läuft nur mit dem Internet Explorer. Da per *JScript* z. B. auch ein Zugriff auf ActiveX-Komponenten möglich wird, ist dieses Feature potentiell gefährlicher als *JavaScript*.

Um die Verwirrung komplett zu machen, gibt es auch noch *VBScript*, ebenfalls eine Microsoft-Spezialität. Hiermit kann man zum Beispiel Webseiten aufpeppen. Allerdings erlaubt *VBScript* den Schreibzugriff auf das System und kann relativ einfach missbraucht werden. Viele Würmer und andere Schädlinge sind in *VBScript* geschrieben. Ein Beispiel haben wir oben im Kapitel „Windows Scripting Host“ auszugsweise gesehen. Mehr ist zu diesem Feature eigentlich nicht zu sagen.

Was tun? Nutzer des Internet Explorers sollten, wie dargestellt, ActiveX deaktivieren. Sie haben weiter das Problem, dass der IE nicht zwischen *JavaScript*, JScript und VBScript unterscheidet. Sie kommen daher nicht umhin, das gesamte Scripting abzuschalten. Eine bebilderte Anleitung, wie man demnach den IE konfigurieren sollte, gibt es hier:

http://www.blafusel.de/ie.html

Nutzer anderer Browser sollten *Java* abstellen. Ganz vorsichtige Menschen verzichten auch auf *JavaScript*.

Mail-Programme

Abschließend noch kurz zu den Mail-Programmen: Ich kann an dieser Stelle keine konkrete Konfigurationsanleitung für jedes gängige Mailprogramm liefern. Hierfür reichen weder der Platz in diesem Thread, noch meine Kenntnisse aller Mailprogramme. Daher nur einige wenige allgemeine Hinweise, spezielleres können wir bei Bedarf im Diskussionsteil besprechen.

Zunächst sollte man darauf verzichten, HTML-Mails zu versenden und zu empfangen. Jedes Mail-Programm bietet die Möglichkeit, HTML abzuschalten, z.B. durch die Option „nur Text“ oder ähnlich. Damit ist man schon einige Sorgen los, da aktive Inhalte wie Scripte nicht ausgeführt werden und sich Schädlinge nicht bei Betrachten der Mails automatisch ausführen können. Außerdem ist zu empfehlen, *Java*, *JavaScript* und das Nachladen von Bildern zu deaktivieren. Letzteres ist zwar kein Sicherheitsrisiko, aber ein Ärgernis, da Spammer durch diese Technik erfahren können, ob eine Mail-Adresse aktiv ist.