E-Maileingang ohne Antivirensoftware säubern

A. Beck

Zusammenfassung

Bericht über einen Versuch den täglich eingehenden Strom an e-Mails in gut und böse einzuteilen. Interessanterweise hat sich die oftmals wenig beachtete, aber einfache Methode der Filterung von e-Mails direkt mit dem e-Mailprogramm als ausgesprochen wirkungsvoll erwiesen, um e-Mails mit Schädlingen im Anhang auszusortieren. Im Laufe von fast zwei Jahren wurden rd. 8.900 e-Mails ohne Antivirensoftware aussortiert. Trotz der Rigorosität der Filterung wurden weder Schädlinge übersehen, noch wichtige e-Mails gelöscht. Auch wenn die Methode nicht für jedermann den Stein der Weisen darstellen mag und sich nicht unbedingt für den Einsatz auf Mailservern eignet, kann sie aber gerade die Computer unbedarfter Endanwender auch vor neuen Varianten wirkungsvoll schützen.

Schlüsselwörter

Antiviren-Software, Computerviren, Trojanische Pferde, Würmer

Einleitung

Waren vor noch nicht allzu langer Zeit Computerschädlinge für viele Nutzer nur wenig mehr als eine theoretische Möglichkeit, gehören heute Berichte über die elektronischen Epidemien (oder sogar Pandemien) in der Tagesschau der ARD eher zum Normalfall. Auch warnen Zeitschriften und Internetportale regelmäßig vor neu auftauchenden Schädlingsvarianten und an Updates für eine ganze Palette von Anti-Virussoftware fehlt es auch nicht. Dennoch wird das Internet nicht sicherer, sondern die Zahl der kursierenden Schädlinge nimmt weiter zu. Die mit Abstand häufigste Art der Verbreitung erfolgt per e-Mail, direkt als Dateianhang an eine e-Mail in das Eingangspostfach des Nutzers.

Genaugenommen stellt sich natürlich die Frage, wieso es immer wieder derart viele Schädlinge schaffen, sich auf den Rechnern der Nutzer breitzumachen, denn von der Theorie her könnten solche Mails umgehend ungeöffnet gelöscht werden. Aber anscheinend ist der Mensch im Allgemeinen zu neugierig um nicht doch ab und zu mal einen Blick in den Anhang zu riskieren. Auch scheint der Einsatz von Anti-Virenprogrammen nicht der Weisheit letzter Schluß zu sein:

- Niemand kann die Fehlerfreiheit von Software garantieren. Dies bedeutet für die Praxis, daß jede installierte Software und jedes Update als potentielle Schwachstelle anzusehen sind.
- Im **günstigsten** Fall kann Anti-Virensoftware immer nur bekannte Schädlinge mit Sicherheit identifizieren. Das Erkennen Neuer bleibt immer mit Unsicherheiten behaftet.
- Update-Zyklen lassen sich nicht beliebig verkürzen. Auch scheint es fraglich ob man die Anwender, die die e-Mails mit den Schädlingen im Anhang schon nicht löschen, dazu bewegen kann im Stundenrhythmus ihre Antivirensoftware, sofern überhaupt vorhanden, mit neuen Daten zu versorgen.

Hier soll nun der Frage nachgegangen werden, ob es nicht einen anderen oder weiteren Ansatz gibt, die Schädlingsfracht in eingehenden e-Mails zu entsorgen. Auch wird das Problem konsequent aus dem Blickwinkel des Anwenders angegangen. Es geht also nicht darum, was Schädlinge anrichten (können), wie sie funktionieren oder woher sie kommen. Für den Anwender ist es im Grunde vollkommen belanglos, welcher Schädling sich bei ihm einnisten will, es muß verhindert werden. Der derzeitige Weg, Schädlinge immer genauer zu klassifizieren und zu differenzieren ist in vieler Hinsicht mehr von akademischem Interesse. Für den Anwender muß es darum gehen möglichst allgemeine, gemeinsame Eigenschaften aufzudecken, an Hand derer er Schädlinge erkennen und aussortieren kann.

Methode

Im Zeitraum vom 31.03.2004 - 31.12.2005 (640 Tage) wurden alle unangekündigten e-Mails mit Anhängen gesammelt, die in irgendeiner Form in den Postfächern der Domäne WWW.Pruefziffernberechnung.DE eingingen. Herkömmliche Spammails (inkl. der Phishing-Mails) blieben unberücksichtigt.

Analyse

Während des Betrachtungszeitraumes trafen insgesamt 8.923 entsprechende e-Mails ein (Tab.1), wobei allein die Anhänge rd. 300 MByte Platz belegen. Das dazugehörige Transfervolumen lag durch den Protokollaufwand und durch die Kodierungen der Anhänge daher noch um einiges höher.

Im Schnitt gab es, trotz einiger punktueller Epidemien, keinen Wochentag an dem permanent besonders viele Schädlingsmails eingingen. Am Wochenende war die Belastung ungefähr halb so groß wie an einem Arbeitstag. Im Schnitt mußte mit 14 Schädlingen pro Tag im Eingangskorb gerechnet werden, die es gilt sicher zu erkennen und zu löschen.

Tabelle 1: Unangemeldete Mails mit Dateianhängen.aufgeschlüsselt nach Wochentagen.
Zeitraum: 31.03.2004 -31.12.2005

Tag	n	Bytes
Montag	1.553	54.635.564
Dienstag	1.651	57.546.403
Mittwoch	1.551	52.322.243
Donnerstag	1.347	42.082.350
Freitag	1.248	40.676.931
Samstag	752	25.650.392
Sonntag	821	26.594.744
∑	**8.923**	**299.508.627**

Faktisch waren alle eingehenden Schädlinge in irgendeiner Form gegen Schwachstellen in Software von bzw. unter MS-Windows gerichtet. Auf Grund der bei den Endanwendern vorherrschenden Monokultur ist dies auch nicht weiter überraschend. Insofern kann man eigentlich kaum noch allgemein von Computerviren reden, sondern muß von Windowsviren sprechen.

Als nächstes wurde versucht der Frage nachzugehen, warum der Anwender die Dateianhänge überhaupt öffnet. Anscheinend erkennt er sie nicht als gefährlich. Eine einfache Methode den Anwender über die wahre Identität einer Datei zu täuschen, besteht darin, den Dateinamen mit mehreren Suffixen (bspw. `.doc`, `.txt`) getrennt durch mehrere (>15) Leerzeichen zu versehen:

```
data.doc                    .pif
document.txt                .exe
```

Der Trick funktioniert aus mehreren Gründen:

- Der Mensch liest oft nur das, was er lesen will und oft nicht bis zum Ende. Im Falle der Beispiele also `data.doc` oder `document.txt`
- In e-Mails stehen öfters einige vermeintlich sinnlose Buchstaben scheinbar zusammenhanglos im Textkörper.
- Ist die Spaltenbreite im Explorer auf eine normale Breite eingestellt, sieht man die durch die Leerzeichen abgetrennte eigentliche Dateierweiterung (`.pif`, `.exe`) einfach nicht.
- Bei allen Anzeigen (Listen, Dialogboxen) bei MS-Windows, gibt es kein gesondertes Feld, in dem immer die wahre Dateiendung angezeigt wird.

Interessanterweise wurde dieser Trick aber nur in 324 von 8.923 (3,63%) Fällen angewandt um vier Dateitypen zu kaschieren (Tab. 2). Der geringe Anteil von unter 4% erklärt somit **nicht** warum Anwender die Anhänge öffnen. Schlüsselt man alle 8.923 Anhänge nach ihren wahren Dateisuffixen auf, ergibt sich ein recht übersichtliches Bild (Tab. 3). Insgesamt sind im betrachteten Zeitraum nur 13 verschiedene Dateiformate eingegangen, wobei der Typ `.zip` mit 39% den Löwenanteil ausmachte. Der größte Teil der Dateianhänge bestand aus Formaten, die wohl nur sehr wenig Bedeutung im regulären Mailverkehr von normalen Anwender haben dürften, bzw. deren Verwendung man vermeiden kann (bspw. kann man Quellcodes von Skripten direkt im Textkörper mailen, anstelle eines Dateianhanges): `.bat`, `.com`, `.cpl`, `.eml`, `.exe`, `.hta`, `.pif`, `.rar`, `.scr`, `.vbs`. Allein diese zehn Dateitypen umfassen 60,5% der ungewollten Dateianhänge. Gelingt es einem, in seinem Mailverkehr diese neun Formate und `.zip` zu vermeiden, schließt man damit auch 99,4% der gesamten Schädlingsfracht aus, ohne auf spezielle Software zurückgreifen zu müssen.

Tabelle 2:
Kaschierte Suffixe

Suffix	n
.exe	56
.htm	1
.pif	199
.scr	68
Σ	**324**

Mailfilter

Wie ein Versuch über mehr als ein Jahr gezeigt hat, ist eine kostenfreie, effektive Mailfilterung tatsächlich möglich, sofern drei Punkte erfüllt werden:

- Verwendung eines e-Mailprogrammes welches automatische Filterung („Regel-Assistent“) erlaubt. Besonders geeignet erweist sich die Filterung mittels regulärer Ausdrücke.
- Information seiner unmittelbaren Umgebung, daß man keine unangekündigten e-Mails mit Dateianhängen (außer vielleicht `.pdf`, `.txt`) mehr akzeptiert.
- Konsequenz! Unangekündigte Anhänge, egal von wem, und von Unbekannten sowieso, werden rigoros gelöscht. Ohne Nachzudenken, ohne Rückfrage!
- Wann immer möglich (z. B. Newsletter), wähle man anstelle von HTML-Mails die Textform. Das ist immer sicherer und schneller.

Die zwar rigorose, aber einfache Möglichkeit besteht nun darin, im e-Mailprogramm einen Filter einzurichten, der nach dem Vorkommen von Suffixen gefährlicher Dateianhänge im Textkörper sucht. In Pseudocode sähe der Filter etwa wie folgt aus:

```
Wenn (Body enthält ".pif") dann
    verschiebe Mail in den Papierkorb
```

Läßt sich mit regulären Ausdrücken arbeiten, müßte ein einfaches Filterkriterium in etwa formuliert werden als:

```
(\.bat)|(\.cpl)|(\.exe)|(\.hta)|
(\.pif)|(\.scr)|(\.vbs)
```

Allein dieser Ausdruck filtert 55,8% alle Schädlinge aus. Welche Dateianhänge ausgefiltert werden können, hängt auch vom Benutzer ab. Wer keine Programme mit anderen per Mail austauscht, kann beruhigt `.exe` wegfiltern. Vorsicht ist geboten beim rigorosen Filtern von `.com`, da es zur Ausfilterung erwünschter Mails führen kann (falsch Positive). Ausgefiltert werden bspw. Mitteilungsmails wie sie von GMX und Web.DE verschickt werden um über Neuzugänge im Spamverdachtsordner zu informieren. Dort werden häufig im Textkörper Listen mit Absender-

adressen verschickt, die Adressen der Art abc@xyz.com enthalten. Ebenso werden URLs des Typs http://WWW.abc.com als falsch positiv bewertet. Wohlgemerkt, der Filter soll nur den Textkörper (Body) nach `.com` filtern, d.h. e-Mails von einer Absenderadresse die auf `.com` endet werden weiterhin empfangen.

Ebenso muß individuell entschieden werden, ob es sinnvoll ist `.zip` zu filtern. Setzt man aber seine Umgebung davon in Kenntnis, daß man keine unangekündigten e-Mails mit Anhängen akzeptiert, kann man beruhigt einen weiteren Filter einrichten:

```
(\.zip)
```

Der Vorteil der Mailfilterung direkt im e-Mailprogramm liegt darin, daß der Filter einmal eingerichtet wird und dann „vergessen“ werden kann. Regelmäßige Updates sind praktisch nicht erforderlich, da auch neue Schädlingsversionen mit dem Suffix einer ausführbaren Datei daherkommen. Der Filter arbeitet sicher im Hintergrund und schafft schädliche Dateien im wahrsten Sinne des Wortes aus dem Blickfeld des Anwenders. Dennoch werden häufige Dateiformate (`.doc`, `.pdf`, `.txt`) in den Anhängen weiter in den Eingangskorb durchgeleitet.

Resümee

Trotz hochkomplizierter Antivirensoftware gelingt es nicht alle e-Mails mit gefährlichen Anhängen auszufiltern. Insbesondere bei neuen Varianten versagt sie oft. Es kommen immer wieder e-Mails durch, die den Anwender zu einem fatalen Klick verleiten. Mit einer rigorosen Filterung nach Dateitypen kann dem durchaus wirkungsvoll begegnet werden.

Welche Zielgruppe eignet sich nun für diese Art der Filterung? Im Grunde können alle Endanwender eine solche Filterung vornehmen. Normalerweise kennt man die Dateien die man regelmäßig benötigt, diese werden dann von der Filterung ausgenommen alles andere gelöscht. Darüber nachdenken sollten auch all diejenigen, die ab und zu in ihrer Umgebung die Rechner von weniger bedarften Bekannten wieder zum Laufen bringen müssen. Oftmals wird gerade dort die Antivirensoftware nicht vom Anwender auf den neuesten Stand gebracht. Der Mailfilter bildet hier durchaus einen wirkunsvollen Schutz, auch vor neuen Varianten und dem Betreuer bleibt die ein oder andere Frage der Art „ich habe hier eine Telekomrechnung erhalten, wie kann ich die öffnen?...“ erspart.

Selbst Anwender die kein MS-Windows verwenden, können von der Mailfilterung profitieren. Da sie mit den meisten Dateianhängen sowieso nichts anfangen können, können sie diese aussortieren. Ein typischer Fall sind hier bspw. Anwender älterer Macs. Das Antivirenprogramm kann hier sogar inzwischen ganz abgeschaltet werden. Die e-Mails mit den entsprechenden Anhängen sind hier nicht gefährlich, sondern einfach nur lästig. Ein Filter im Mailprogramm löst das Problem recht elegant.

Tabelle 3: Unangemeldete Mails mit Dateianhängen, aufgeschlüsselt nach Suffixen

Suffix	n		Bytes					
		%	Summe	$\bar{X}$	σ	Minimum	Maximum	%
.bat	202	2,3 %	11.370.630	56.290	5.758	2.222	91.856	3,8 %
.bmp	28	0,3 %	85.616	3.058	1.129	1.794	4.766	0,0 %
.com	423	4,7 %	14.505.710	34.292	17.109	4.278	56.808	4,8 %
.cpl	218	2,4 %	5.254.258	24.102	4.292	204	40.687	1,8 %
.eml	1	0,0 %	2.403	-	-	2.403	2.403	0,0 %
.exe	434	4,9 %	11.231.328	25.879	7.649	4.653	106.613	3,7 %
.hta	45	0,5 %	3.757.000	83.489	24.425	70.131	137.356	1,3 %
.htm	20	0,2 %	21.885	1.094	1.174	38	5.515	0,0 %
.pif	2.215	24,8 %	55.708.778	25.151	11.119	1	62.464	18,6 %
.rar	1	0,0 %	18.080	-	-	18.080	18.080	0,0 %
.scr	1.775	19,9 %	55.183.015	31.089	9.794	486	152.064	18,4 %
.vbs	92	1,0 %	7.763.088	84.381	25.648	68.939	135.789	2,6 %
.zip	3.469	38,9 %	134.606.836	38.803	22.210	0	1.000.000	44,9 %
Σ	**8.923**	**99,9 %**	**299.508.627**	**33.566**	**18.971**	**0**	**1.000.000**	**99,9 %**