

COMPUTERVIREN/ COMPUTERSCHÄDLINGE

Stand: 23.05.2006

VORWORT:	3
1. <u>WAS SIND COMPUTERSCHÄDLINGE?</u>	3
2. <u>WELCHE ARTEN VON COMPUTERSCHÄDLINGEN GIBT ES?</u>	5
2.1 BOOTSEKTORVIREN	5
2.2 PROGRAMMVIREN	5
2.3 MAKROVIREN/WÜRMER (SKRIPTVIREN)	6
2.4 TROJANISCHE PFERDE	6
2.5 MALICIOUS CODE	6
3. <u>WIE VERMEHREN SICH COMPUTERSCHÄDLINGE?</u>	8
3.1 BOOTSEKTORVIREN	8
3.2 PROGRAMMVIREN	8
3.3 MAKROVIREN/WÜRMER (SKRIPTVIREN)	8
3.4 TROJANISCHE PFERDE	9
3.5 MALICIOUS CODE	9
4. <u>WORAN KANN MAN COMPUTERSCHÄDLINGE ERKENNEN?</u>	10
5. <u>WIE KANN MAN SICH VOR COMPUTERSCHÄDLINGEN SCHÜTZEN?</u>	11
6. <u>WAS TUN, WENN EIN COMPUTER BEREITS MIT EINEM SCHÄDLING INFIZIERT IST?</u>	11
7. <u>WAS BEDEUTET „IN THE WILD“?</u>	12
8. <u>WAS SIND „HOAXES“?</u>	12
9. <u>NAMENS GEBUNG VON SCHÄDLINGEN:</u>	13

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

<u>10. VERHALTENSMAßREGELN ZUM SCHUTZ VOR SCHÄDLINGEN:</u>	<u>14</u>
<u>11. WAS IST SONST NOCH INTERESSANT ZU WISSEN?</u>	<u>16</u>
<u>12. REVIEW 2002:</u>	<u>18</u>
<u>13. REVIEW 2003:</u>	<u>20</u>
<u>14. REVIEW 2004:</u>	<u>21</u>
<u>15. REVIEW 2005:</u>	<u>22</u>
<u>16. WEITERFÜHRENDE INFORMATIONEN/LITERATURNACHWEIS:</u>	<u>23</u>
<u>17. HAFTUNGS AUSSCHLUß/DISCLAIMER:</u>	<u>25</u>

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

Vorwort:

Die Begriffe Virus und Wurm werden in der Fachliteratur häufig äquivalent benutzt. Dies ist technisch nicht korrekt. Allerdings hat sich der Begriff Computervirus als Beschreibung für alle Arten von Computerschädlingen durchgesetzt. Dabei ist der Unterschied zwischen Viren und Würmern gering:

Analog zur Biologie benötigen Viren einen Wirt, während Würmer autark agieren [1], [2].

Für Computer bedeutet das, daß Viren ein Dokument (z.B. eine Word- oder Exceldatei) benötigen. Als Wirte können aber auch Programme fungieren, z.B. kleine Tools oder Bildschirmschoner, welche man sich aus dem Internet heruntergeladen hat. Würmer stellen dagegen eigenständige Programme oder Skripte dar. Viele Würmer kommen in Form von VBS-Skripten (VB = Visual Basic), per E-Mail-Anhang ans Ziel und benötigen den standardmäßig vorhandenen Windows Scripting Host (WSH).

Für den normalen Anwender ist die Unterscheidung nach Virus oder Wurm relativ unwichtig. Wenn einer zugeschlagen hat, spielt dies keine Rolle mehr. Für den Fachmann, der das Problem beseitigen muß, ist diese Unterscheidung aber möglicherweise von Relevanz. Die richtige Umschreibung für dieses Problem ist daher „Computerschädling“! Letztendlich trägt die Software zur Bekämpfung von Computerschädlingen auch den Namen „Virenschanner“, obwohl diese Software selbstverständlich auch Würmer und Trojaner beiseitigen kann. In diesem Aufsatz wird nach Möglichkeit der korrekte Begriff Computerschädling verwendet.

1. Was sind Computerschädlinge?

Computerschädlinge sind normale Programme oder anderweitig direkt ausführbare Codes (Skripte). Im Gegensatz zu beispielsweise Textverarbeitungsprogrammen besitzen Schädlinge keine „nützlichen“ Befehle. Statt zum Beispiel Funktionen für die Texterstellung anzubieten, lösen sie in der Regel sogenannte „Schadensfunktionen“ [3] aus. Schadensfunktionen können sich auf verschiedenste Art und Weise zeigen.

Offensichtliche Schadensfunktionen sind z.B.:

- das Löschen der Festplatte (Verlust aller Daten und Programme des Datenträgers),
- das Verhindern der Ausführung eines Programms,
- das Verändern von Daten, z.B. von Texten oder Tabellen,

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

- das Löschen des BIOS-Bausteins,
- das Versenden von Dokumenten per E-Mail,
- die Überlastung von Netzwerken durch Reproduktion (Weiterverbreitung),
- die hohe Auslastung von Computersystemen durch die Weiterverbreitung,
- das Ausspähen von Daten (z.B. eBay Paßwörter, Online Banking PIN/TAN etc.),
- usw.

Schadensfunktionen gibt es unüberschaubar viele. Oftmals gelangen sie in diversen Kombinationen durch einen Schädling zur Anwendung. Zur Zeit gibt es je nach Art der Zählweise zwischen 20.000 und 115.000 Computerviren. Pro Monat kommen etwa 200-500 neue hinzu. Die verschiedenen Zahlenangaben hängen davon ab, ob man Virenfamilien zusammenfaßt oder jede Variante einzeln zählt. Man muß dabei bedenken, daß „polymorphe“ Viren bei jeder Infektion ihren Programmcode verändern und daher - streng genommen - einen neuen Virus (neue Variante) darstellen. Echte Schadensfunktionen, die den Verlust von Daten des Anwenders verursachen, sind bei den Schädlingen der letzten 3-5 Jahre immer seltener zu beobachten. Mittlerweile sind bei modernen Schädlingen zwei Funktionen vorherrschend: erstens die schnelle Reproduktion (Weiterverbreitung) von Schädlingen und zweitens das Ausspähen von allerlei Zugangsdaten. Dies führt zu zusätzlichen Problemen, da die Struktur des Internets durch die extreme Verbreitungsgeschwindigkeit der Schädlinge belastet wird. Dann können z.B. einzelne Webseiten nicht mehr abrufbar sein, oder E-Mail-Server überlastet werden. Welchen Stellenwert gestohlene Online-Banking PIN/TANs haben oder ein entführter eBay-Account, kann man dann an seinem Kontostand erkennen.

Zusammenfassung:

Computerschädlinge sind Programme, die verschiedenartige Schäden an den Daten oder der Hardware anrichten. Viele neuere Schädlinge der letzten Jahre beschränken sich allerdings darauf, sich „nur“ weiterzuverbreiten. Beliebt ist derzeit das Stehlen von Zugangsdaten.

2. Welche Arten von Computerschädlingen gibt es?

Grundsätzlich kann man folgende Hauptarten [1], [2] von Schädlingen unterscheiden:

- 2.1 Bootsekturviren
- 2.2 Programmviren
- 2.3 Makroviren/Würmer (Skriptviren)
- 2.4 Trojanische Pferde und
- 2.5 Malicious Code

Innerhalb dieser Hauptarten werden einige Varianten unterschieden [2], [3]:

- normale Viren
- stealth Viren (Tarnkappenviren)
- polymorphe Viren
- usw

2.1 Bootsekturviren

Bootsekturviren sind die einfachste Virenform. Diese Viren ersetzen den auf jeder Diskette, Festplatte oder sonstigen Datenträgern vorhandenen Bootcode durch einen neuen Bootcode. Bei jedem Einschalten eines Computers wird am Anfang der Bootcode (z.B. von der Festplatte) ausgelesen und abgearbeitet. Der Bootcode enthält Anweisungen, wo auf der Festplatte das Betriebssystem zu finden ist, bzw. wie dieses gestartet wird. Ein Bootsektorvirus ergänzt diesen Bootcode beispielsweise mit dem Befehl, die Festplatte zu formatieren. Dies bewirkt den Verlust aller auf dieser Festplatte gespeicherten Daten.

2.2 Programmviren

Programmviren funktionieren ähnlich wie Bootsekturviren, nur daß sie nicht den Bootsektor angreifen, sondern ausführbare Dateien, also Programme. Ein Programmvirus ergänzt also EXE- bzw. COM-Dateien um bestimmte Befehle, die beim Starten des infizierten Programms die Schadensfunktionen ausführen.

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

2.3 Makroviren/Würmer (Skriptviren)

Makroviren/Würmer sind neue, sehr effektive und weit verbreitete Schädlinge. Der erste Makrovirus [4] ist etwa 1995 aufgetaucht und hat damals ausschließlich Word-Dokumente befallen. Heute haben Makroviren und Würmer von allen Schädlingsarten die größte Verbreitung erreicht. Ihre Anzahl nimmt weiter rapide zu, da sie von allen Schädlingen am einfachsten zu programmieren sind und kaum tiefergehende Kenntnisse einer Programmiersprache erfordern.

Schädlinge dieser Art können theoretisch alle Programme befallen, die in der Lage sind, eine Makrosprache (Skriptsprache) auszuführen. Am bekanntesten sind die E-Mail-Programme Outlook und Outlook Express in Kombination mit dem „Windows Scripting Host“ (WSH), dicht gefolgt von Word und Excel. Es gibt aber auch Skripte für spezielle Programme wie AutoCad oder Adobe Acrobat (nicht Acrobat Reader!). Bekannt geworden sind „Melissa“ [5] und „I love you“ [6], [7].

2001 zeichnete sich durch eine Revolution bei den Schädlingen aus, die zweite Hälfte des Jahres 2001 brachte bislang die größte Flut von Makroviren und Würmern mit sich. Namen wie „Nimda“ [8] und „CodeRed“ [9] werden wohl in die Annalen der Computerviren-Geschichte eingehen. Alle diese Schädlinge stehen für ein neues Verbreitungskonzept auf dem Computerviren-Markt und können als die ersten echten Internetviren bezeichnet werden, da sie in der Lage sind, Webseiten (Webserver) zu befallen. Ebenso dramatisch ist die Entwicklung von Würmern wie: „SirCam“ [10] und „BadTrans“ [11], die dadurch bekannt wurden, daß sie Dokumente des Anwenders per E-Mail versenden.

2.4 Trojanische Pferde

Trojanische Pferde sind eigentlich nützliche Programme, die aber ein zweites gefährliches Programm mit einschleppen. Der Begriff wird fast immer in Zusammenhang mit sogenannten „Backdoors“ - also Hintertüren - verwendet. Hintertüren sind in der Regel Programme, die es einem Angreifer erlauben, infizierte Rechner fernzusteuern - so als ob er selbst an der Tastatur säße. Somit kann der Angreifer alles tun, was man selbst auch tun kann. Weiterhin werden sehr oft Spionageprogramme mit Hilfe eines Trojanischen Pferdes eingeschleust. Diese Spionagesoftware ist in der Lage, Paßwörter und Zugangsdaten (z.B. fürs Online-Banking oder T-Online) auszuspähen und einem Angreifer weiterzuleiten. Teilweise werden auch ganz banale Viren per Trojanischem Pferd eingeschleust. Beispiele sind: BackOrifice [12] und SubSeven [13].

2.5 Malicious Code

Als „Malicious Code“ werden zerstörerische Befehle in Internetseiten bezeichnet. Da es möglich ist, direkt in Webseiten Skript-Befehle einzubauen, werden diese, ent-

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

sprechend der Sicherheitseinstellungen des verwendeten Browsers, beim Öffnen einer Webseite aktiv. Mit diesen Befehlen ist alles möglich: vom Anzeigen sinnloser Meldungen, über das Öffnen unendlich vieler Browserfenster bis zum Formatieren der Festplatte. Seit Ende 2003 sind diese Schädlinge verstärkt anzutreffen. Leider haben fast alle derzeitig zur Verfügung stehenden Browser (IE, Netscape, Opera, etc.) Sicherheitslücken, die sich durch Malicious Code besonders einfach ausnutzen lassen. Einige dieser Lücken, besonders beim Internet Explorer (IE), sind schon länger bekannt und immer noch nicht geschlossen worden [14]. Hier ist Microsoft in der Verantwortung, endlich etwas gegen die zahlreichen Probleme zu unternehmen.

Varianten:

- Normale Viren sind Viren, die nicht über besondere Eigenschaften verfügen. Zum Beispiel keine Maßnahmen treffen, einen Virens scanner zu überlisten.
- Stealth Viren sind in der Lage, ihre Anwesenheit vor einem Virens scanner zu verbergen.
- Polymorphe Viren können ihren eigenen Programmcode bei jeder neuen Infektion verändern. Dadurch sind sie durch herkömmliche Virens scanner kaum zu erkennen.

Zusammenfassung:

Es gibt verschiedene Hauptarten von Schädlingen, die man in mehrere Untervarianten aufgliedert. Die Untervarianten dienen meistens dazu, den Schädling selbst zu schützen und sein Überleben zu sichern. Während die alten Plagen wie Bootsektorviren und Programm viren langsam aussterben, steigt die Gefahr durch die neuen Vertreter dieser Spezies, die Makroviren und Würmer, rasant. Fast wöchentlich erscheinen neue und neuartige Schädlinge mit teils katastrophalen Ausmaßen.

Bootsektorviren gibt es zwar noch, der letzte neue Virus dieser Gattung wurde allerdings 1998 entdeckt [15].

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

3. Wie vermehren sich Computerschädlinge?

Je nach der Art eines Schädlings kommen verschiedene Möglichkeiten der Ausbreitung [16] in Frage.

3.1 Bootsektoviren

Ein Bootsektorvirus wird beim Booten eines Rechners aktiv. Einmal in den Arbeitsspeicher eines Computers gelangt, wartet er dort im Hintergrund ab, bis man einen neuen Datenträger einlegt. Wenn man also eine Diskette in ein Laufwerk einlegt und darauf zugreift, erkennt dies der Virus und tauscht den Bootcode der Diskette aus. Damit sich der Virus von der infizierten Diskette aus fortpflanzen kann (um weitere Computer zu schädigen), muß von dieser Diskette gebootet werden. Auch wenn die Diskette gar kein Betriebssystem besitzt, das gestartet werden könnte, ist der Bootvirus ab diesem fehlgeschlagenen Bootversuch aktiv, und die Festplatte eines Computers wird infiziert. Eine einfache und 100%ig wirksame Gegenmaßnahme ist, im BIOS die Bootreihenfolge derart zu verändern, daß ein Booten von Diskette nicht möglich ist.

3.2 Programmviren

Programmiviren funktionieren ähnlich wie Bootsektorviren und pflanzen sich auch ähnlich fort. Sie sind, einmal aufgerufen, im Hintergrund aktiv und infizieren jede neue ausführbare Datei, die gestartet wird. Da sehr oft Programme auf CDs oder über das Internet weitergegeben werden, sind alle Voraussetzungen erfüllt, sich einen solchen Virus einzufangen.

3.3 Makroviren/Würmer (Skriptviren)

Sie sind die gefährlichsten Schädlinge. Sie nisten sich z.B. in Word- oder Excel-Dateien ein. Beim Aufruf eines infizierten Dokumentes schreiben sie sich in die globale Dateivorlage dieser Programme. Da die globale Dateivorlage beim Starten von Word oder Excel standardmäßig geladen wird, sind sie sofort im Hauptspeicher aktiv und infizieren jedes neu angelegte oder geöffnete Dokument.

Mittlerweile ist der „Windows Scripting Host“ (WSH) auf jedem neuem Windows-System installiert. Daher verwenden immer mehr Würmer dieses Programm als Basis, dessen Zweck das Ausführen von Makros (Skripten) ist. WSH-Skripte (zu erkennen an den Dateiendungen .vbs und .js) erschließen sich über den WSH beinahe alle Funktionen des zugrunde liegenden Betriebssystems.

Mitte 2001 tauchte der „Nimda“-Wurm [8] auf. Er nutzt eine neue Verbreitungsform. Nimda ist der erste Wurm, der Internetseiten/Internetserver infizieren kann. Mit dem

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

Browser im Internet zu surfen reicht aus, um ein Opfer dieses Wurms zu werden. Mittlerweile gibt es viele Ableger des Nimda-Wurms.

Fast alle neuen Schädlinge seit Ende 2001 sind Würmer und basieren oft auf VBS.

3.4 Trojanische Pferde

Trojanische Pferde benötigen, um als Computerschädling ans Ziel zu gelangen, die gleiche Unterstützung wie das geschichtliche Original. Ohne das Zutun des Benutzers sind sie harmlos.

Trojanische Pferde werden aktiv, indem der Benutzer es selbst ausführt. Natürlich weiß der Benutzer nicht, daß es sich um ein Trojanisches Pferd handelt. Das Trojanische Pferd verbreitet sich, indem der Anwender z.B. von einer Internetseite ein vermeintlich nützliches Programm herunterlädt und dieses ausführt. Dabei kann es sich auch um einen Bildschirmschoner o.ä. handeln. Besonders beliebt sind Programme, die Freischaltcodes für Microsoft-Produkte oder pornografische Internetseiten illegal generieren.

3.5 Malicious Code

Malicious Code verbreitet sich in der Regel nicht selbst. Er wird von unfreundlichen Menschen in deren Webseiten eingebaut und gelangt zur Ausführung, sobald der unbedarfte Surfer diese Webseiten aufruft. (Prinzipiell könnte man den Nimda-Wurm auch als Malicious Code bezeichnen, da er sich in Webseiten einbindet. So einfach ist es bei Nimda dann aber doch nicht, er benötigt dazu die Hilfe des Webservers, von dem er sich auf Grund eines Fehlers im IIS* ausführen läßt).

* (er kann nur den Microsoft Internet Information Server (IIS) befallen)

Seit 2004 befallen zahlreiche neue Schädlinge (IIS-basierte) Webserver und fügen den „guten“ Seiten den schädlichen Malicious Code hinzu, mit teilweise gravierenden Folgen für den arglosen Surfer [17].

Zusammenfassung:

Während Schädlinge sich früher vorwiegend durch den Austausch von Disketten vermehrt haben, verbreiten sie sich mittlerweile vorwiegend durch das Internet. Besonders E-Mail-Attachments sind, wegen zu laxer Sicherheitseinstellungen, die größte Gefahr. Dies hat „I love you“ [6], [7] eindrucksvoll demonstriert. Auch sollte man sich nicht in Sicherheit wiegen, wenn man kein Windows benutzt. Ein Schädling wie „I love you“ ist genauso unter Linux und unter MacOS möglich [18].

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

Mit „Nimda“ wurde eine neue Runde in der Virentechnologie eingeläutet. Die Frage lautet nicht, ob man jemals ein Virenopfer wird, sondern wann. Das ständig zunehmende Auftreten von mit Malicious Code manipulierten Webseiten verschärft dieses Problem erheblich.

4. Woran kann man Computerschädlinge erkennen?

Computerschädlinge erkennt man meistens erst dann, wenn es bereits zu spät ist. Wer seinen Computer einschaltet und vom BIOS nur noch die lapidare Meldung „kein System- oder fehlerhafte Diskette“ erhält und somit eine gelöschte oder formatierte Festplatte vorfindet, kann nur noch hoffen, daß die letzte Datensicherung in Ordnung ist. Bloß: Wie lange liegt die zurück? 1 Tag, 1 Monat, 1 Jahr ?

Gelöschte Festplatten, Programme oder Dateien sind nur eine mögliche Ursache, an der man einen Schädling erkennt. Verdächtig ist auch, wenn der Computer ungewöhnlich langsam arbeitet, oder seltsame Dinge passieren, z.B. nervöses Aufflackern von Dialogfenstern oder heftige Aktivität des E-Mail-Programms.

Wer anormales Verhalten erkennt, ist vielleicht noch in der Lage, einen Virenscanner einzusetzen, wenn aber z.B. einfach aus dem Nichts eine Meldung erscheint, man soll einen bestimmten Satz eingeben oder die Festplatte würde gelöscht, ist es meistens sinnvoll, dieser Aufforderung nachzukommen [19]. Wer seinen Computer in diesem Moment einfach abschaltet, hat bereits verloren. Der Schädling hat zu diesem Zeitpunkt den Bootsektor und/oder die Dateien auf der Festplatte bereits verschlüsselt - und nur noch professionelle Datenretter können an diesem Zustand etwas ändern, dabei entstehen jedoch Kosten in Höhe von mehreren Tausend Euro.

Die einfachste Methode, einen Schädling zu erkennen, ist immer noch der Einsatz eines Virenscanners. Wichtig ist, daß er aktuell ist. Ein 3 Wochen alter Virenscanner ist praktisch nutzlos.

Zusammenfassung:

Schädlinge erkennt man in der Regel erst, wenn sie ihr schändliches Werk bereits vollendet haben. Daher ist es wichtig, seinen Computer regelmäßig mit einem neuen Virenscanner zu untersuchen und in regelmäßigen, kurzen Intervallen Backups der Daten anzulegen.

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

5. Wie kann man sich vor Computerschädlingen schützen?

Ganz einfach: niemals eine fremde CD ins eigene Laufwerk einlegen und um jeden Internetanschluß einen großen Bogen machen! Das dies jedoch nicht im Sinne des Erfinders ist, dürfte jedem klar sein. Daher gilt: Immer einen aktuellen Virens Scanner einsetzen, dessen Signaturen nicht älter als 1 Tag sein sollten. Weiterhin jede fremde Diskette und CD vor dem ersten Zugriff mit dem Virens Scanner überprüfen. Auch USB Sticks und Digitalkameras(!) sollte man nicht vergessen, auch diese sind Datenträger, die Schädlinge enthalten können. Am besten man scannt diese manuell, ohne sich auf das Wächtermodul des Virens Scanners zu verlassen. Diese ständig im Hintergrund aktiven Wächtermodule sind zwar gut, aber eine manuelle Prüfung kann trotzdem den einen oder anderen Schädling finden, den das Wächtermodul übersieht. Natürlich gilt das auch für Dateien und Programme, die man sich aus dem Internet heruntergeladen hat.

Auch Originaldisketten und CDs vom Hersteller sind leider nicht unbedingt virenfrei [20], [21], [22], [23].

Darüber hinaus sollte man seine Daten in regelmäßigen Abständen sichern. Dies ist nicht nur wegen Computerschädlingen ratsam, sondern auch wegen der Gefahr eines Festplattendefektes.

Zusammenfassung:

Entweder nie eine fremde CD in den eigenen Computer einlegen bzw. aus dem Internet Programme herunterladen oder aber fremde Daten und Programme vor dem ersten Zugriff mit einem aktuellen Virens Scanner prüfen.

6. Was tun, wenn ein Computer bereits mit einem Schädling infiziert ist?

Besteht der Verdacht, daß der Computer mit einem Schädling infiziert ist, gilt folgendes:

Als erstes die Arbeit wie üblich beenden und den Computer ausschalten. Alle Verbindungen zu anderen Computern trennen, indem man das Netzkabel entfernt bzw. das ISDN-, oder Modemkabel. Den Computer von einer 100%ig virenfreien Bootdiskette/CD [24] starten und mit einem Virens Scanner überprüfen. Am besten ist, den Virens Scanner dabei auch von Diskette oder CD zu starten. Wer sich seiner Sache nicht sicher ist, sollte jemanden fragen, der sich auskennt, oder z.B. im Rechenzentrum der nächsten Hochschule nach Hilfe fragen. Meist gibt es an Hochschulen Mitarbeiter, die nur für die Rechnersicherheit und somit auch für die Schädlingsab-

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

wehr zuständig sind. Allerdings stellen einige Hochschulen Dienste dieser Art für externe Anwender mittlerweile in Rechnung.

Das Internet ist eine weitere Informationsquelle. Wer in einer der bekannten Suchmaschinen das Stichwort „Viren“ oder präziser „Computerviren“ eingibt, wird garantiert fündig.

Zusammenfassung:

Wer einen Schädling auf dem Rechner hat, sollte von einer garantiert virenfreien Diskette oder CD booten und danach den Rechner mit einem aktuellen Virenschanner überprüfen. Vorsicht bei PCs mit Windows XP oder Windows 2000. Zwar sind laut Werbeaussage alle Virenschanner in der Lage, auch im von CD gestarteten Zustand diese Systeme zu untersuchen, leider stimmt dies gerade bei den beiden am weitesten verbreiteten Produkten definitiv nicht [25].

7. Was bedeutet „In the Wild“?

Es gibt derzeit etwa 115.000 verschiedene (bekannte) Schädlinge. Die Wahrscheinlichkeit, jeden dieser Schädlinge aber tatsächlich einmal auf dem eigenen Rechner anzutreffen, ist gering. Deshalb unterscheidet man „In the Wild“-Viren und „In the Zoo“-Viren. Es gibt nur wenige hundert Viren mit wirklich nennenswerter Verbreitung [26], [27]. Der überwiegende Teil der bekannten Schädlinge sind „In the Zoo“-Viren - also Schädlinge hinterm Zaun. Sie existieren fast nur in Laboren der namhaften Antivirus-Software-Hersteller und bilden nahezu keine Gefahr mehr. Sie sind meist als „Proof-of-Concept“-Projekt entstanden oder sind veraltet und können sich nicht weiter verbreiten.

Zusammenfassung:

Nur von „In the Wild“-Viren geht eine reale Gefahr aus. „In the Zoo“-Viren gibt es fast nur im Labor.

8. Was sind „Hoaxes“?

„Hoaxes“ [28] sind womöglich die gemeinsten, aber auch ungefährlichsten Schädlinge. Schlicht und einfach gesagt: „Hoaxes“ sind „Witze“. Diese „Schädlinge“ sind bekannt geworden durch den „Good Times“-Hoax. Zur Anfangszeit der massenhaften

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

Internetbegeisterung ging eine E-Mail um die Welt, in der vor dem Betreff „Good Times“ gewarnt wurde. Der Inhalt war etwa folgender:

„Warnung vor einer E-Mail mit der Betreffzeile Good Times. Das Lesen einer E-Mail mit dem Betreff Good Times reicht aus, um Ihre Festplatte zu löschen. Öffnen Sie daher eine E-Mail mit diesem Betreff auf keinen Fall, und schicken Sie diese Warnung an alle Ihre Bekannten und Freunde weiter.“

Wichtig ist hierbei der Satz: *„...und schicken Sie diese Warnung an alle Ihre Bekannten und Freunde weiter.“* Ein Hinweis mit der Aufforderung zum Weiterleiten ist typisch für eine „Hoax“-Mail.

Dies ist auch schon der ganze Virus. Eine E-Mail mit dem Betreff „Good Times“ kann also bedenkenlos gelesen werden, sofern man sie sofort als Hoax identifiziert.

Nach neueren Ansichten wird jedoch der Standpunkt vertreten, daß eigentlich auch von Hoaxes eine Gefahr ausgeht. Denn egal was ein Schädling tut, am Ende entsteht immer ein finanzieller Schaden. Auch durch einen Hoax entsteht ein finanzieller Schaden durch den bloßen Verlust an Arbeitszeit, die durch die Beschäftigung mit diesem Thema verloren geht. Die Zeit zum Schreiben dieses Abschnitts ist der direkte Beweis für diese Theorie. 10 Minuten, die womöglich für etwas anderes besser investiert worden wären.

Beispiele für Hoaxes sind: Jdbgmgr [29], [30] und Sulfnbk [31], [32].

Zusammenfassung:

„Hoaxes“ sind schlechte Witze, deren einziger Schaden der Verbrauch von Arbeitszeit ist.

9. Namensgebung von Schädlingen:

Ein Virus - viele Namen! Obwohl eine Konvention [33] zur Benennung von Schädlingen besteht, trägt ein Schädling bei jedem Hersteller einen anderen Namen, was natürlich verwirrend sein kann. Schädlinge sollten prinzipiell nach der „1991 News Virus Naming Convention“ (NVNC '91) benannt sein, welche 1999 durch die GSNC '99 aktualisiert wurde [33]. Hier nur einige beispielhafte Bedeutungen von wichtigen Begriffen, die man bei Schädlingsbezeichnungen antrifft:

- I = I-Worm (Wurm, der sich über das Internet verbreitet)
- W32 = Win32 (Schädling, der 32Bit-Windows-Betriebssysteme befällt)
- VBS = Visual Basic Script (Virus/Wurm, der in VBS programmiert wurde)
- @MM = Massmailer (Schädling, der sich massiv per E-Mail weiterverbreitet)

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

X97M = Excel 97 Makro Virus (Virus, der Excel 97 befällt)

Somit beschreibt die Bezeichnung: „W97M.Assilem.B“ einen Virus Namens „Assilem“, der „Word 97“ befällt. Es ist ein „Makro“-Virus und liegt in der Variante „B“ vor.

In Zukunft soll ein gänzlich neues Schema zur Anwendung kommen [33].

10. Verhaltensmaßregeln zum Schutz vor Schädlingen:

Der beste und wirksamste Schutz gegen Computerschädlinge ist das richtige Verhalten des Anwenders beim Surfen und im Umgang mit E-Mails. Hierzu sind folgende wenige Verhaltensregeln wichtig:

- Verwenden Sie einen sichereren Browser (z.B. Opera), oder konfigurieren Sie den Internet Explorer auf höhere/maximale Sicherheit. Einbußen bei der Darstellung von Webseiten sind dabei hinzunehmen. Wichtige Internetseiten können in die Zone für vertrauenswürdige Seiten aufgenommen werden.
- Verwenden Sie ein sichereres E-Mail Programm (z.B. Pegasus), oder konfigurieren Sie Outlook (Express) auf maximale Sicherheit.
- Sorgen Sie dafür, daß stets die aktuell verfügbaren Sicherheitsupdates des Betriebssystems und der Anwendersoftware auf Ihrem PC installiert sind.
- Öffnen Sie keine E-Mails mit Anhang, wenn Sie diesen nicht erwartet oder angefordert haben. Insbesondere Anhänge mit den Dateierendungen .jpg, .exe, .pif, .com, .bat, .scr und .vbs sind als bedrohlich einzustufen [34], aber auch Word- und Excel-Dateien sowie PowerPoint-Präsentationen können Schädlinge in Form von Makroviren enthalten. Jpg-Dateien - also Bilder – sind die neuesten Problemfälle. Sorgen Sie dafür, daß Ihre Kommunikationspartner Ihnen möglichst PDF-Dokumente zusenden, und verschicken auch Sie selbst möglichst nur PDF-Dateien. Sollten dennoch Office-Dokumente versendet werden, dann besteht bislang die größte Sicherheit bei der Wahl des Dateiformats RTF (Rich Text Format) bei Word und CSV bei Excel.
- Wenn Sie in Ihrem E-Mail-Programm bei den Anhängen keine Dateierendung sehen (z.B. .doc, .xls ...), sollten Sie dringend diese Voreinstellung von Windows ändern. Sie laufen sonst Gefahr, daß Sie an einen Schädling geraten, der sich mit einer doppelten Dateierendung tarnt (z.B. .doc.pif).
- Löschen Sie E-Mails ungelesen, deren Betreffzeile unsinnig ist (z.B. Re: That movie).

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

- Löschen Sie fremdsprachige E-Mails von Absendern, mit denen Sie üblicherweise auf deutsch kommunizieren, ungelesen.
- Löschen Sie E-Mails mit kleinen Unterhaltungsprogrammen wie z.B. dem Mohrruhn ungelesen.
- Löschen Sie generell E-Mails, die Ihnen irgendwie seltsam vorkommen, ungelesen.
- Schalten Sie die automatische Voransicht ihres E-Mail-Programms ab – vor allem dann, wenn Sie Outlook oder Outlook Express benutzen.
- Wenn Sie sich nicht sicher sind, ziehen Sie Hilfe zu Rate.
- Wenn es Sie dann doch erwischt hat, trennen Sie sofort den Rechner vom Netzwerk/Internet (Kabel abziehen) und holen sich fachliche Unterstützung.
- Beschuldigen Sie niemals denjenigen, der als Absender einer infizierten E-Mail eingetragen ist. Die meisten modernen Schädlinge tarnen sich mit fremden oder gefälschten Absendern.
- Wenn Sie eine E-Mail erhalten, die Sie vor einem neuen gefährlichen Virus warnt und die Sie an alle Ihre Freunde und Bekannten weiterleiten sollen, löschen Sie diese. Sie sollten diese E-Mail unter keinen Umständen an andere Personen weiterleiten, in der Regel ist dies eine „Hoax“-Mail. Wenn Sie nicht ganz bewußt einen entsprechenden „Newsletter“ dazu abonniert haben, werden Sie niemals per E-Mail Virenwarnungen erhalten. Insbesondere Firmen wie z.B. Microsoft, IBM, usw. versenden keine Warnungen per E-Mail.
- Ziehen Sie in Erwägung, eine „Personal-“ oder „Desktop-“ Firewall zu installieren, wenn Sie mit der Funktionsweise dieser Software und den Netzwerktechnologien intensiv vertraut sind. Wenn Sie eine Personal Firewall einsetzen, ohne die Hintergründe wirklich zu verstehen, ist der mögliche Schaden allerdings größer als der Nutzen!

Weiteres hierzu unter: www.ingbuero-klarmann.de/downloads/firewall-information.pdf.

- Informieren Sie sich möglichst täglich über einen IT-Newsticker im Internet wie z.B. www.heise.de. Gefährliche Viren und Würmer werden dort aktuell gemeldet, sobald der Ausbruch bekannt wird.
- Computerschädlingen ist es egal, ob Sie eine Standleitung oder ob Sie nur ein langsames Modem zur Verfügung haben.

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

- Wenn Sie auf das Internet angewiesen sind bzw. einen Großteil Ihrer Arbeit über das Internet abgewickelt wird, dann sollten Sie einen Fortbildungskurs zum Thema „IT-Sicherheit für Anwender“ besuchen.

Zusammenfassung:

Das richtige Verhalten ist der beste und effektivste Schutz vor Computerschädlingen. Anders ausgedrückt: Keine noch so gute Schutzsoftware ist in der Lage, Ihnen zu helfen, wenn Sie sich falsch verhalten!

11. Was ist sonst noch interessant zu wissen?

- Besondere Virus Formen: Der CIH-Virus [35]

Der CIH-Virus nimmt eine absolute Ausnahmestellung unter den Viren ein. Er ist in der Lage, einen Computer grundlegend zu schädigen. Bis zum Erscheinen des CIH-Virus war der schlimmste Schaden eines Virus das Löschen der Partitionstabelle der Festplatte. Passiert das, dann heißt es: Festplatte neu partitionieren, Betriebssystem und Programme neu installieren, Datensicherung zurückspielen und nach einigen Stunden Arbeit geht wieder alles. CIH ist anders. CIH ist in der Lage, den BIOS-Baustein bestimmter Motherboards zu löschen (Bei CIH betrifft es nur Boards mit Intels TX Chipsatz). Wenn dies der Fall ist, kann der Computer nicht mehr gestartet werden. Abhilfe besteht nur durch den Kauf eines neuen BIOS-Bausteins oder durch das Neubeschreiben des alten. Zum Neubeschreiben müssen allerdings ein zweiter Computer sowie eine spezielle Steckkarte vorhanden sein. Steht kein neues BIOS zur Verfügung, ist der Computer (bzw. das Motherboard) nicht mehr verwendbar. Sollte man keinen Computer mit TX-Chipsatz besitzen, löscht CIH „nur“ die Partitionstabelle.

Ein weiterer BIOS-Killer ist der W32/Kriz-Virus [36]: er schlägt immer am 25. Dezember zu und zerstört laut PC Professionell: „... *das CMOS-RAM und das Flash-BIOS, löscht Daten auf der Festplatte*“ - also ein ganz übler Kandidat! Der W32/Kriz ist nicht auf den TX-Chipsatz beschränkt.

Wenn man die Entwicklung solcher Viren wie z.B. den CIH sieht, ist es eigentlich nur noch eine Frage der Zeit, bis Viren noch mehr können. Beispiel: Bei vielen aktuellen Grafikkarten kann man die Taktfrequenz per Software einstellen [37]. Ein entsprechender Schädling könnte dann die Taktrate des Grafikprozessors höher setzen. Ergebnis: Der Grafikchip brennt durch, und es werden bis zu 1000 Euro für eine neue Grafikkarte fällig.

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

- Wer einen Schädling auf seinem Rechner findet, sollte alle Freunde und Geschäftspartner warnen, mit denen er in der letzten Zeit Dokumente (per E-Mail oder CD usw.) od. ä. ausgetauscht hat. Aber bitte telefonisch!
- Regelmäßiges Überprüfen mit einem aktuellen Virens Scanner ist eine der wichtigsten Waffen im Kampf gegen Computerschädlinge.
- Nicht alle Schädlinge sind gefährlich, einige verstehen sich „nur“ als Scherzprogramm. Wer sich aber darauf verläßt, schadet sich und seiner Umwelt.
- Befolgen Sie die Verhaltensmaßregeln aus Kapitel 10.

Überblick über Antivirus-Software-Hersteller (ohne Wertung der Qualität):

- McAfee (Network Associates) <http://www.mcafee.de>
- Trend Micro <http://www.trendmicro.de>
- Norman Data Defense <http://www.norman.de>
- Promus conception <http://www.promus.de>
- Symantec (Norton Antivirus) <http://www.symantec.de>
- F-Secure (ehemals Percomp Verlag) <http://www.f-secure.com>
- G-Data <http://www.gdata.de>
- H+B EDV Datentechnik <http://www.antivir.de>
- AntiVir Personal Edition (kostenloser Scanner von H+B EDV Datentechnik) <http://www.free-av.de>
- Kaspersky <http://www.kaspersky.com/de/>

Viele der hier aufgeführten Firmen bieten im Internet zeitlich begrenzte Demoversionen zum kostenlosen Download an.

Weitere Internet-Adressen:

- AV-Test (Führt Tests von Virens Scannern durch): <http://www.av-test.de>
- c't Antivirus Informationen: <http://www.heise.de/security/dienste/antivirus/>

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

- c't Browsercheck (Sicherheit testen):
<http://www.heise.de/security/dienste/browsercheck/>
- c't E-Mailcheck (Sicherheit testen):
<http://www.heise.de/security/dienste/emailcheck>
- Heise Security: <http://www.heisec.de>
- Network Associates Virendatenbank: <http://vil.nai.com>
- Bundesamt für Sicherheit in der Informationstechnik: <http://www.bsi.de>
- Informationen des BSI für Privatleute: <http://www.bsi-fuer-buerger.de>
- Hoax-Infoseiten der TU Berlin (mit aktueller Hoax-Liste):
<http://www.tu-berlin.de/www/software/hoax.shtml>
- Virus Bulletin (Unabhängige Viren-Informationen): <http://www.virusbtn.com>
- Wildlist (welche Viren sind im Umlauf?):
<http://www.virusbtn.com/resources/wildlists>
- eicar (Anti-Virus test file): http://www.eicar.org/anti_virus_test_file.htm
- Virenkalender: http://vil.nai.com/vil/calendar/virus_calendar.aspx
- Risiko Einstufung von Computerschädlingen:
http://www.networkassociates.com/de/security/resources/risk_assessment.htm

12. Review 2002:

Bis auf einzelne Ausnahmen gegen Ende des Jahres war 2002 ziemlich ruhig. Erheblich ruhiger als erwartet, was sogar die Branche der Antivirus-Software-Hersteller zu entsprechenden Pressemeldungen verleitete [38]. (Dafür kamen im Januar 2003 gleich mehrere Schädlinge in geballter Form. Hervorzuheben zum Beispiel W32.Sobig [39] und mit katastrophalen Auswirkungen: SQL-Slammer [40]).

Der Trend weg von den Viren und hin zu Würmern setzte sich fort. Fast alle hervorstechenden Schädlinge in 2002 waren Würmer. Diese Würmer waren zunehmend in der Lage, selbständig Webserver zu befallen. Auffallend hieran war, daß alle diese Schäden vermeidbar gewesen wären. Alle diese Würmer (selbst Nimda als erster seiner Unterart) basieren auf Sicherheitslücken von Webservern, die lange vorher bekannt waren und für die schon geraume Zeit Patches (Korrekturen) bereitstanden.

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

Im Prinzip liegt damit eine Mitschuld bei den zuständigen Administratoren dieser Server. Beim SQL-Slammer verhält es sich ähnlich, der Fehler im SQL-Server 2000 ist schon lange bekannt, und entsprechende Korrekturen sind längst verfügbar gewesen.

Auch war 2002 festzustellen, daß (langsam aber stetig) auch Linux zum Angriffsziel wird. Einige Würmer haben (lange bekannte) Lücken dieses Systems ausgenutzt um sich zu verbreiten. Auch hier tragen die Administratoren die Verantwortung. Betroffen ist der am weitesten verbreitete Webserver Apache [41], [42].

Leider werden die gerne gekauften Virens Scanner für Heimanwender immer schlechter! Entweder sind ihre Erkennungsraten indiskutabel niedrig, oder die Benutzeroberfläche ist so umständlich, daß die Produkte falsch konfiguriert werden. Dazu kommen erhebliche Probleme dieser Produkte im Zusammenspiel mit modernen NT-basierten Betriebssystemen wie Windows XP. Diese Produkte wurden für die DOS-basierte Windows 9x/ME Generation entwickelt, die nicht mehr vertrieben wird. Ganz langsam stellen sich die Hersteller auf die gravierenden Unterschiede bei Windows 2000 und XP ein [43].

Als Folge bleibt nur übrig, auch dem Heimanwender professionelle Virens Scanner (Corporate-Versionen) ans Herz zu legen. Diese sind allerdings um ein Vielfaches teurer und für Privatleute schwierig zu beschaffen.

Während es früher ausreichte, einmal im Monat die Virensignaturen zu aktualisieren, sollte man dies mittlerweile stündlich machen. Das Problem hierbei: Viele Hersteller stellen nur wöchentlich oder bei akuter Gefahr neue Signaturen bereit. Wer aber auf den Internetseiten der Hersteller sucht, wird meistens gut versteckt (immerhin) täglich aktualisierte Signaturen finden. Zum Beispiel für NAI/McAfee* unter: [44].

* Seit März 2005 liefert McAfee für Corporate Versionen standardmäßig tägliche Updates [45].

Ein weiterer wichtiger Aspekt ist die Anzahl der eingesetzten Virens Scanner. Nicht allein aufgrund eines Gerichtsurteils [46], [47] ist der Einsatz mehrerer unterschiedlicher Virens Scanner sinnvoll. Allerdings ergeben sich dabei zuweilen technische Schwierigkeiten. Zwei oder mehr Virens Scanner gleichzeitig auf einem PC sind höchst problematisch. Als guter Kompromiß bietet es sich an, auf dem eigenen PC einen Virens Scanner einzusetzen und für den E-Mail-Verkehr einen Provider zu suchen, auf dessen Servern auch nach Viren gesucht wird [48]. Es ist dabei lediglich sicherzustellen, daß der Provider ein anderes Produkt benutzt. Optimal wäre natürlich, wenn dazu noch ein eigener Gateway- und SMTP-Scanner käme. Für Anwender mit 1 oder 2 PCs ist der Aufwand hierfür in der Regel zu groß. Dies läßt sich meist nur in größeren Netzwerkstrukturen realisieren.

Die sogenannte Heuristikfunktion von Virens Scannern, die in der Lage sein soll, auch neue, bislang unbekannte Viren anhand bestimmter Kriterien zu erkennen, ist mei-

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

stens unbrauchbar [43], da sie der Komplexität moderner Schädlinge nicht gerecht wird.

13. Review 2003:

Außer im Januar 2003 (siehe Kapitel 12) hat es im August 2003 wieder mal so „richtig gekracht“. Um den 12. bzw. 19. August herum haben die Schädlinge W32.Blaster/Lovesan [49], [50] und W32.Sobig.F [51] innerhalb kürzester Zeit alle Rekorde gebrochen [52], [53]. Das Verbreitungstempo war ungeahnt hoch, und für den Schädling „Blaster“ gilt wieder mal: Die Sicherheitslücke und die entsprechende Fehlerbereinigung („Patch“) waren Wochen vorher bekannt! [54], [55], [56], [57].

Blaster stellte hierbei noch einmal eindrucksvoll die Gefährlichkeit von sogenannten „Buffer Overflows“ heraus [58], [59]. Die Virenscanner waren zwar in der Lage, den vollständigen Befall des Computers durch Blaster zu verhindern, dies aber erst nachdem sie aktualisiert wurden. Den reinen Angriff auf den Computer konnten und können sie aber nicht abfangen. Das Neustarten des PC oder den Absturz des „Svhost“ kann man damit nicht verhindern. Um sich hiervor zu schützen, sind regelmäßig die verfügbaren Windows-Updates zu installieren und/oder weitere technische Maßnahmen zu ergreifen [60], [61].

Muß man zu Sobig.F noch etwas schreiben? Vielleicht eines: Die Sobig-Schädlinge haben die interessante Eigenschaft, über ein Verfallsdatum zu verfügen [62]. Sobald also ein Sobig-Schädling abläuft, kann kurz darauf mit dem nächsten gerechnet werden. Der ursprüngliche Sobig.F läuft am 10. September ab, mal sehen was also Sobig.G in diesem Jahr noch alles anrichten wird...

Ein weiterer Trend sind Schädlinge, die sich explizit über die bekannten Tauschbörsen wie Kaaza, eDonkey etc. verbreiten. Auch die beliebten Messenger von Yahoo, Microsoft, AOL etc. werden zunehmend zum Ziel speziell darauf angepaßter Schädlinge.

Stellt sich die Frage, ob die Gesetzgeber in aller Welt einen verbindlichen „Internet- oder Computersicherheits-Führerschein“ einführen sollten? Wer die Möglichkeit hat, sollte auf jeden Fall entsprechende Seminare besuchen, das Geld hierfür ist gut angelegt – vielleicht sogar besser als auf dem Bankkonto! Wenn sich wirklich herausstellen sollte, daß Blaster zumindest eine Teilschuld an dem großen Stromausfall im Nordosten der Vereinigten Staaten besitzt, erwischt es als nächstes vielleicht die Geldinstitute [63].

Zum Linnegraben 46	Telefon: +49 (069) 395955	E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

14. Review 2004:

Im Jahr 2004 war besonders auffällig, daß sich viele Schädlinge besonders an deutschsprachige Anwender richten. Die „Sober“-Schädlinge zum Beispiel [64], [65], deren Variante „Sober.C“ [66] besonders perfide mit Ermittlungen der Düsseldorfer Staatsanwaltschaft gegen den Empfänger der infizierten E-Mail droht [67].

Am 27. Januar wurde ich in einem Interview bei Rhein-Main-TV gefragt, ob 2004 „der“ Supervirus erscheint. Anlaß war der am Tag zuvor ausgebrochene Mydoom.A Schädling [68]. Es schien zwar ein wirklich heftiges Virenjahr zu werden, aber mit einem sog. Supervirus war nicht zu rechnen. Dann traten im Februar 2004 drei gravierende Ereignisse ein, die sicherlich eine neue Qualität im Bereich der Computerschädlinge darstellen. Erstens begann eine ca. 12 Wochen lange Phase, in der praktisch täglich neue, sehr extreme Viren verbreitet wurden. Die Basisnamen: MyDoom, Bagle und Netsky [69], [70]. Hintergrund war ein Schlagabtausch einiger Schädlings-Programmierer untereinander [71]. Einer dieser Programmierer wurde dann wegen eines weiteren extremen Schädlings namens „Sasser“ in Deutschland verhaftet [72]. Zweitens wurden im Februar Teile des Windows-Quellcodes gestohlen und veröffentlicht [73]. Es dauerte nur drei Tage, bis darin die erste Sicherheitslücke gefunden wurde [74]. Seitdem sind auch Bitmapdateien (BMP) als gefährlich einzustufen – bis dahin eines der harmlosesten Dateiformate überhaupt. Drittens veränderte sich die Art und Weise, wie sich einige dieser Schädlinge verbreiten. Um sich vor Virenschernern zu schützen, versenden sie sich als verschlüsseltes ZIP-Archiv per E-Mail und verlangen vom Anwender ganz frech die Eingabe des Paßwortes, welches in der Mail enthalten ist.

Nach diesen Vorfällen kamen wieder einmal Forderungen nach einem Computerführerschein auf.

Und was ist mit dem Supervirus? Nun, es gibt ihn tatsächlich! Im Trouble um MyDoom, Bagle, Netsky und Sasser hat sich, von der Öffentlichkeit weitgehend unbekannt, Phatbot [75] auf den Computern von zahlreichen Anwendern breit gemacht. Phatbot ist der Prototyp des Supervirus. Phatbot nutzt nahezu alle derzeit bekannten Verbreitungsmethoden und Sicherheitslücken. Er ist flexibel entworfen und modular erweiterbar. Er liegt, und das ist das Gravierende, im Quellcode vor und hat ein unüberschaubares Schadenspotential.

Haben Sie von Phatbot noch nichts gehört, wo es doch „der“ Supervirus ist? Das ist genau das tückische an einem Supervirus. Er verrichtet sein Werk heimlich, still und leise im Hintergrund, während er das gesamte Schadenspotential von Computerschädlingen in einem Programm vereint. Zu einem Zeitpunkt x könnte Phatbot oder einer seiner Nachfolger noch Schlagzeilen machen. Das liegt dann aber nicht im Interesse der ursprünglichen Programmierer, sondern wohl eher wieder an streitenden Jugendlichen.

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

Während eher „harmlose“ Schädlinge wie Sasser [76] Schlagzeilen machen, kann man mit Schädlingen der Kategorie Phatbot Geld verdienen [77].

Gegen Ende des Jahres kristallisierte sich die nächste Richtungsänderung bei den Computerschädlingen heraus:

- Während bislang zerstörungswütige Jugendliche als Virenschreiber galten, steigt jetzt das organisierte Verbrechen in die Thematik ein [78].
- Es sind fast ausnahmslos „Kombi-Schädlinge“ aktiv – also Schädlinge, die eine Kombination aus Viren, Würmern und Trojanischen Pferden darstellen.
- Zum Hauptverbreitungsweg E-Mail gesellen sich in großem Maße manipulierte Webseiten hinzu [79], [80].
- Es findet eine Vermischung mit weiteren Sicherheitsproblemen statt: Phishing, Adware, Spyware und reguläre Schädlinge arbeiten Hand in Hand [79].

Zudem verschärft sich das Problem mit den Reaktionszeiten der Antivirus-Software-Hersteller [81]. Einige Virens Scanner werden noch immer nicht den Anforderungen von Windows 2000 und Windows XP gerecht [43], [78]. Das Service Pack 2 für Windows XP geht in die richtige Richtung, ist aber auf halbem Wege stehengeblieben. Noch immer macht es Windows den Schädlingen leichter als nötig. Unter anderem auch deshalb, weil für viele Anwender immer noch die Bequemlichkeit wichtiger ist als die Sicherheit.

Für 2005 bedeutet all dies nichts Gutes:

- Windows hat weiterhin katastrophale Lücken.
- Die Beseitigung von Windowslücken dauert immer noch zu lange.
- Die Virens Scanner sind nicht unbedingt besser geworden.
- Die Update-Zyklen vieler Virens Scanner dauern zu lange.
- Die Schädlinge werden immer raffinierter.
- Zusätzliche Sicherheitsprobleme verschärfen das Sicherheitsdilemma.

Fazit: Das Surfen und Mailen gleicht einem Lauf durchs Minenfeld.

15. Review 2005:

Was gab es Neues im Jahr 2005? Nun im Prinzip das, was sich Ende 2004 bereits abgezeichnet hat. Computerschädlinge dienen den Autoren der Schadsoftware zum Geldverdienen, und die neuen Varianten haben an Bedeutung zugenommen. In erster Linie ist hier das Phishing zu nennen [82]. Phishing ist ein Kunstbegriff und setzt sich zusammen aus Password und Fishing. Es bedeutet soviel wie Paßwörter fischen oder einfach ausgedrückt das heimliche Ausspähen von allerart Zugangsdaten. Allerart meint dies auch so, wobei der Schwerpunkt auf dem Ergaunern von PINs und TANs fürs Onlinebanking liegt. Die Konsequenz sind somit leereräumte Bankkonten. Die Kosten, welche durch den fahrlässigen Umgang mit moderner Informationstechnik entstehen, werden somit auch für Privat-Anwender real spürbar.

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	E-Mail: oliver.klarmann@ingbuero-klarmann.de
---	---	--

Leider machen es viele Unternehmen den Phishern unangemessen leicht.

Als Faustregel zum Schutz vor Phishing-Mails gilt: Keine Bank oder z.B. eBay wird jemals per E-Mail zum Bestätigen der Zugangsdaten auffordern. Insbesondere Mails, die freundlicherweise gleich einen Link zur Registerseite enthalten, sind sofort zu löschen. Der Link sieht zwar korrekt aus, weist in der Regel aber auf eine gefälschte Kopie der eigentlichen Seite hin. Den Link zu seiner Bank sollte man immer aus den Favoriten aufrufen oder manuell in die Adreßzeile seines Browsers eintragen.

Weitere Hilfe ist zu finden unter: <https://www.a-i3.org/>

16. Weiterführende Informationen/Literaturnachweis:

- [1] <http://www.heise.de/security/dienste/antivirus/typen.shtml>
- [2] <http://www.cms.hu-berlin.de/publikationen/dl/software/viren/arten.htm>
- [3] <http://www.bsi.bund.de/literat/faltbl/index.htm>
- [4] <http://www.bsi.de/av/vb/concept.htm>
- [5] <http://www.bsi.de/av/vb/melissa.htm>
- [6] http://vil.nai.com/vil/content/v_98617.htm
- [7] <http://www.heise.de/newsticker/data/mst-04.05.00-001/>
- [8] <http://www.bsi.de/av/vb/nimda.htm>
- [9] <http://www.bsi.de/av/vb/codered.htm>
- [10] <http://www.bsi.de/av/vb/sircam.htm>
- [11] <http://www.bsi.de/av/vb/badtransb.htm>
- [12] <http://www.bsi.de/av/vb/backori.htm>
- [13] <http://www.bsi.de/av/vb/subseven.htm>
- [14] <http://www.heise.de/newsticker/meldung/46474>
- [15] Korrespondenz des Autors mit Network Associates (McAfee)
<http://www.mcafee.de/>
- [16] <http://www.cms.hu-berlin.de/publikationen/dl/software/viren/>
- [17] <http://www.heise.de/security/artikel/48622>
- [18] <http://www.heise.de/newsticker/data/jk-14.05.00-000/>
- [19] <http://antivirus.perwein.com/viren/geschichte.htm>
- [20] <http://www.heise.de/newsticker/data/pab-06.07.01-000/>
- [21] <http://www.heise.de/newsticker/data/tol-17.06.02-001/>
- [22] <http://www.heise.de/newsticker/data/ps-24.04.01-000/>
- [23] <http://www.heise.de/newsticker/data/ghi-09.04.99-000//>
- [24] siehe Heft CD zu c't 19/2004
- [25] c't 03/2004 Seite 122ff und c't 01/2005 Seite 128ff.
- [26] <http://www.virusbtn.com/resources/wildlists/>
- [27] <http://www.wildlist.org/>
- [28] <http://www.tu-berlin.de/www/software/hoax.shtml>
- [29] <http://www.tu-berlin.de/www/software/hoax/jdbgmgr.shtml>
- [30] http://www.bsi.bund.de/av/hoaxes/hoax_jdb.htm
- [31] <http://www.tu-berlin.de/www/software/hoax/sulfnbk.shtml>

Zum Linnegraben 46 Telefon: +49 (069) 395955 E-Mail: oliver.klarmann@ingbuero-klarmann.de
65933 Frankfurt am Main Fax: +49 (069) 38013651
Mobil: +49 (0179) 2001336

- [32] <http://www.bsi.bund.de/av/hoaxes/sulfnbk.htm>
- [33] ix 09/2002 Seite 93
- [34] PC Professionell 10/2003 Seite 172ff
- [35] http://vil.nai.com/vil/content/v_10300.htm
- [36] http://vil.nai.com/vil/content/v_10255.htm
- [37] http://www.de.tomshardware.com/graphic/19991019/geforce256_ocing-02.html#uumbertakten_des_geforce_256
- [38] <http://www.heise.de/newsticker/data/ku-25.08.02-001/>
- [39] <http://www.heise.de/newsticker/data/pab-14.01.03-000/>
- [40] <http://www.heise.de/newsticker/data/pab-25.01.03-000/>
- [41] <http://www.netcraft.com/>
- [42] <http://www.heise.de/newsticker/data/hag-14.09.02-002/>
- [43] c't 25/2002 Seite 192ff.
- [44] <http://vil.nai.com/vil/stinger/default.aspx>
- [45] <http://www.heise.de/security/news/meldung/56378>
- [46] <http://www.heise.de/newsticker/data/pab-14.08.01-000/>
- [47] <http://www.internet4jurists.at/sonstiges/viren1a.htm>
- [48] z.B. Schlund und Partner
<http://www.schlund.de/>
- [49] <http://www.heise.de/security/news/meldung/39358>
- [50] <http://www.heise.de/newsticker/data/dab-12.08.03-000/>
- [51] <http://www.heise.de/newsticker/data/pab-19.08.03-000/>
- [52] <http://www.heise.de/newsticker/data/dab-20.08.03-001/>
- [53] <http://www.message-labs.com/emailthreats/default.asp>
- [54] <http://www.heise.de/security/artikel/39389>
- [55] <http://www.heise.de/newsticker/data/dab-17.07.03-000/>
- [56] <http://www.heise.de/newsticker/data/ju-25.07.03-001/>
- [57] PC Professionell 10/2003 Seite 42
- [58] <http://www.heise.de/security/artikel/37958>
- [59] <http://www.heise.de/security/artikel/38982>
- [60] <http://www.microsoft.com/technet/security/current.aspx>
- [61] <http://www.ingbuero-klarmann.de/downloads/firewall-information.pdf>
- [62] http://vil.nai.com/vil/content/v_100561.htm
- [63] <http://www.heise.de/security/artikel/39578>
- [64] <http://www.heise.de/newsticker/data/dab-27.10.03-001/>
- [65] <http://www.heise.de/newsticker/data/dab-28.10.03-000/>
- [66] http://vil.nai.com/vil/content/v_100912.htm
- [67] <http://www.heise.de/newsticker/data/dab-22.12.03-002/>
- [68] <http://www.heise.de/newsticker/meldung/44035>
- [69] <http://www.heise.de/newsticker/meldung/43768>
- [70] <http://www.heise.de/newsticker/meldung/44765>
- [71] PC Professionell 05/2004 Seite 14ff.
- [72] <http://www.heise.de/newsticker/meldung/47205>
- [73] <http://www.heise.de/newsticker/meldung/44586>
- [74] <http://www.heise.de/newsticker/meldung/44690>
- [75] <http://www.heise.de/newsticker/meldung/46634>
- [76] <http://www.heise.de/newsticker/meldung/47037>
- [77] c't 05/2004 Seite 18ff
- [78] c't 01/2005 Seite 124ff, 128ff und 138ff
- [79] <http://www.heise.de/security/artikel/49687>
- [80] <http://www.heise.de/security/news/meldung/54714>
- [81] c't 08/2004 Seite 168
- [82] <http://www.heise.de/newsticker/meldung/55724>

17. Haftungsausschluß/Disclaimer:

Aufgrund der Schnellebigkeit und Innovationsfreude der IT-Branche kann keine Gewähr für die Richtigkeit und Dauerhaftigkeit dieser Informationen gegeben werden. Es bestehen keine Haftungsansprüche gegen den Autor, wenn durch Fehler im Text Kosten entstanden sind. Für die Informationen der weiterführenden Links wird keine Haftung übernommen.

Es ist gestattet, dieses Skript oder Teile davon für eigene Zwecke wie Schulungen etc. einzusetzen, sofern Sie einen Hinweis auf den Autor und die Bezugsquelle lesbar anbringen.

© Dipl.-Ing. Oliver Klarmann, Frankfurt am Main 1997-2006, Computer Viren Information Version 14b