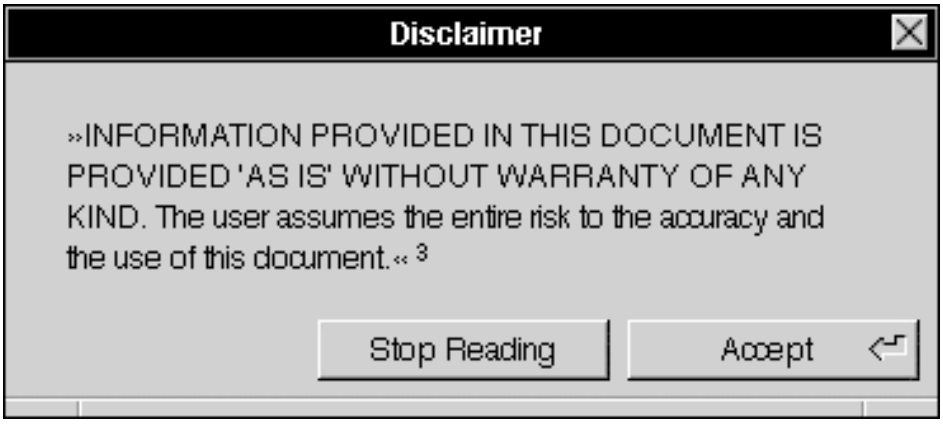
FAQ: Microsoft

Jörg Pflüger und Peter Purgathofer

Es könnte im folgenden der Eindruck entstehen, daß wir keine Sympathisanten von Microsoft sind. Dieser Eindruck täuscht nicht. Tatsächlich glauben wir, daß die Praktiken des Software-Giganten aus Redmond eine Gefahr für die Entwicklung der Informationstechnologie und der selbstbestimmten Nutzung ihrer Errungenschaften darstellen. Um dies zu belegen, wollen wir einige Problemfelder exemplarisch vorstellen. Wir haben dazu die Form eines FAQs[1] (»Frequently Asked Questions«) gewählt – in der Computerkultur die verbreitetste Form der Vermittlung von schlichten Weisheiten. Die angeführten Exempel stellen nur einen kleinen Ausschnitt der im Web diskutierten Probleme mit Microsoft dar; wir haben sie ausgewählt, weil sie uns interessant erscheinen und weil sie auch in ihren technischen Tücken einigermaßen gut erklärbar sind.[2] Da sich die Taktiken von Microsoft häufig ändern, auch wenn ihr strategisches Ziel der weltweiten Vorherrschaft im IT-Bereich gleich bleibt, kann es sein, daß einige Behauptungen nicht (mehr) zutreffen. Wir nehmen deshalb mit dem folgenden Disclaimer das gleiche Recht wie Microsoft in seinen Veröffentlichungen und Lizenzen in Anspruch.



[1] »FAQ /F-A-Q/ or /fak/ n. [Usenet] 1. A Frequently Asked Question. 2. A compendium of accumulated lore, posted periodically to high-volume newsgroups in an attempt to forestall such questions.« [88]

[2] Aus Platzgründen können wir wichtige Aspekte hier nicht behandeln, z.B. Microsofts eigenwilliges Lizenzgebahren [59] [9] [37], ihre vielen schlecht benutzbaren Programme in inkompatiblen Versionen oder Microsofts .NET-Initiative und den damit einhergehenden Kampf mit AOL um die Kontrolle des Zugangs zu Content und Services im Web [16].

Es sei ausdrücklich darauf hingewiesen, daß viele der beschriebenen Praktiken nicht das alleinige ›Vorrecht‹ von Microsoft sind, sondern auch von anderen Konzernen wie beispielsweise Adobe oder AOL gepflegt werden. Besonders gefährlich sind sie, wenn sie von einem Monopolisten betrieben werden, und Microsoft ist aus diesem Grunde in den USA verurteilt worden.

[3] Dieser Haftungsausschluß findet sich beispielsweise in Microsofts Viren-Warnung nach Ausbruch der »I Love You«-Epidemie. [82] Wir haben dazu die Fenstergestaltung von NeXTstep, einem Betriebssystem aus dem Jahre 1988, gewählt, um eine weitere ›Inspirationsquelle‹ für das seit Windows 95 ›charakteristische‹ Windows-Design zu zeigen.

Fragen:

1. Werden durch Beschränkungen von Microsoft tatsächlich Innovationen in der Informationstechnologie verhindert?
2. Wie kann Microsoft mit technischen Mitteln andere Entwickler behindern oder gar ausschließen?
3. Was ist von Microsofts Sicherheitsinitiative zu halten?
4. Wieso gibt es denn bei Microsoftprodukten so viele Sicherheitsprobleme?
5. Wie reagiert Microsoft auf publik gewordene Sicherheitsmängel?
6. Wie hält es Microsoft mit der Privatsphäre der Nutzer?
7. Wie steht Microsoft zu Open Source?
8. Was bedeutet FUD?
9. Wieso können Firmen so schlechte Software vertreiben?
10. Wo soll das alles enden?

---

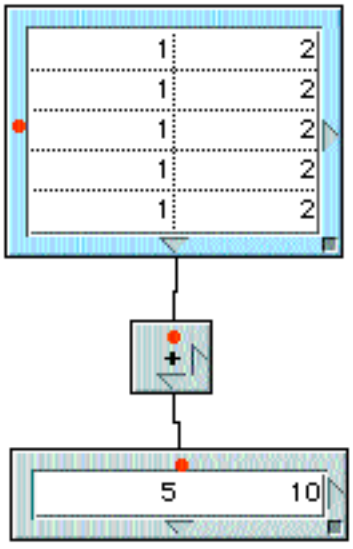
1. Werden durch Beschränkungen von Microsoft tatsächlich Innovationen in der Informationstechnologie verhindert?

Microsoft verteidigt vehement ein ›Recht auf Innovation‹, das aus ihrer Sicht der Freiheit, nach Belieben Schalten und Walten zu können, gleich kommt. Im aktuellen Microsoft-Verfahren wurde behauptet, die von den neun US-Bundesstaaten geforderte Modularisierung des Betriebssystems würde Windows zerstören, und Microsofts Chief Executive Officer (CEO) Steve Ballmer hat gar angedroht, gegebenenfalls Entwicklung und Vertrieb einzustellen.[4] Nun ist es legitim zu fragen, welchem Ziel Microsofts Innovationen dienen und wem sie zu Nutzen sind: Helfen sie dem Nutzer, besser und effektiver mit dem Computer arbeiten zu können, oder helfen sie Microsoft, ihre Marktmacht auszubauen und ihr Monopol bei Betriebssystemen auf andere Bereiche auszudehnen?

[4] »I actually think we would need to withdraw the Windows product from the marketplace. That ... would be the only way I understand to comply with the proposal as put forward by the non-settling states«. [121] Weniger lächerlich war die Ankündigung von Bill Gates in seiner Zeugenaussage vom 22. April 2002, daß die geforderte Modularisierung von Windows zu unbenutzbaren Rumpfbetriebssytemen führen würde. [40] Es ist zwar kein technischer Grund dafür einzusehen, aber eine potentielle Firmenstrategie zu erkennen. Später mußte Gates zugeben, daß ein modular aufgebautes Windows XP durchaus machbar ist. [48a]

Als erstes kann man feststellen, daß allein schon durch die von Microsoft mit allen Mitteln verteidigte Monopolstellung Innovationen anderer Entwickler verhindert oder verdrängt werden. In einigen Anwendungsbereichen haben Softwareanbieter die Entwicklung weitgehend eingestellt oder ihre Produkte vom Markt genommen, etwa bei Spreadsheets (wg. Excel) und bei Präsentationssoftware (wg. Powerpoint).[5]

Spreadsheets stellen prinzipiell problematische Gebilde dar. Sie sind vollwertige Programmiersprachen, unter dem Gesichtspunkt der Kontrolle dessen, was man tut, jedoch denkbar schlechte, weil man nur schwer überschauen kann, was eine Verknüpfung von Operationen bewirkt. Wenn man bedenkt, wieviel Geld mit Excel verwaltet wird, wären bessere Möglichkeiten der Kontrolle und Übersicht dringend geboten. Aber Excel, dessen grundsätzliches Konzept sich nach wie vor an das erste Spreadsheet, VisiCalc von Dan Bricklin und Bob Frankson aus dem Jahre 1979, anlehnt und es im wesentlichen nur um immer mehr, für die meisten Nutzer überflüssige Funktionen anreichert, verhindert durch seine Marktbeherrschung innovative Alternativen. Versucht haben es zum Beispiel Cassady & Green 1996 mit der visuellen Kalkulations-Software »Let's Keep It Simple Spreadsheet«, die genau genommen kein Spreadsheet, sondern eine objektorientierte Programmierumgebung war. Statt Zahlen und Formeln wie üblich in einem großen, zweidimensionalen Raster unterzubringen, sind Tabellen, Ergebnisse und Operationen hier selbständige Objekte, die durch Formeln verbunden und anschaulich dargestellt werden.



	A	B
1	1	2
2	1	2
3	1	2
4	1	2
5	1	2
6	5	10

Links: die Summation zweier Spalten in einem sehr einfachen ›Let's Keep It Simple Spreadsheet‹-Dokument; die Relation von Daten und Ergebnis wird durch den sichtbaren Operator und die Verbindungen transparent.

Rechts: die gleiche Summation in Excel, wo die Unsichtbarkeit der Formeln die Zusammenhänge der sichtbaren Zahlen ›verdunkelt‹.

[5] Die verbliebenen ernstzunehmenden ›Konkurrenten‹ in diesem Bereich sind Open-Source Projekte (z. B. Open Office), weil deren Fortbestand nicht vom finanziellen Erfolg einer Herstellerfirma abhängt. Leider fehlt solchen Projekten zumeist ein einheitliches Konzept des User Interfaces, und es werden allzuoft Microsoft-Produkte imitiert. Echte Innovationen für den Endnutzer, d.h. neue Konzepte, die die Arbeit wesentlich verändern oder gar verbessern könnten, sind auch hier nicht zu erkennen.

Ein Review aus dem Jahr 1996 ist von der neuen Technologie begeistert: »you can set up an error-free spreadsheet in about one-third the time it would take in Excel.« [108] Im gleichen Absatz wird aber auch darauf hingewiesen, daß das Produkt aufgrund der marktbeherrschenden Stellung von Excel nahezu chancenlos ist. Bei dessen Marktanteil von 95% herrscht im Bereich Kalkulationssoftware eine Monokultur, in der es weder Wettbewerb noch Konkurrenz für Microsoft gibt, – und damit auch keinen Anreiz für Innovationen, die nur auf dem Boden einer konkurrierenden Vielfalt gedeihen können.

Microsoft selbst ist nicht gerade für konzeptionelle und technische Innovationen berühmt. Eric Raymond, einer der bekanntesten ›Evangelisten‹ der Open-Source Community (-> 7.), steht mit seiner »Anti-Microsoft Jeremiade« durchaus nicht allein: »Bill Gates pretends to defend “innovation", and if he did I'd love him for it. But there's very little evidence that Microsoft even knows what the word means. Buying or outright stealing key technologies rather than innovating has been a Microsoft trait from the beginning. Consider this list... MS-DOS: bought (from Tim Paterson). PC1 BIOS code: stolen (almost bit-for-bit from Gary Kildall's CP/M BIOS). The Windows interface: copied (incompetently, from Apple). On-the-fly disk compression: stolen (from Stac Electronics). Internet Explorer: bought or stolen, depending on who you believe (from Spyglass). And the list only *starts* with these. And the worst -- the absolute *worst* -- is that he's conditioned computer users to expect and even *love* derivative, shoddily-implemented crap. Millions of people think that it's right, it's *normal* to have an operating system so fragile that it hangs [or] crashes three or four times a week and has to be rebooted every time you change anything deeper than the wallpaper. Dammit, we knew how to do better than that in 1975!« [93] [6]

Manchen Lesern mögen Raymonds Lamentationen überzogen erscheinen, und leider können wir auf deren Berechtigung hier nicht näher eingehen.[7] Wir benügen uns mit einem Hinweis auf Microsofts Vorstellung vom Umgang mit ihren Produkten: In den »Microsoft Inductive User Interface Guidelines« ist folgende Empfehlung für die Gestaltung einer ›guten‹ Benutzeroberfläche zu finden: »A well-designed inductive interface helps users answer two fundamental questions they face when looking at a screen: What am I supposed to do now? Where do I go from here to accomplish my next task?« [76] Diese Richtlinie, die davon ausgeht, Nutzer müßten sich bei der Arbeit am Computer laufend fragen, was man denn von ihnen verlangt, gibt einen Einblick in die (Ab-)Gründe vieler schlecht zu benutzender Programme: Es wird ein Verhältnis zwischen Computer und Nutzer zugrundegelegt, bei dem der Computer das Sagen hat.

---

[6] Bill Gates sieht das vermutlich anders; allerdings ist zu bemerken, daß er in seiner Aussage im aktuellen Prozeßverfahren in dem langen Abschnitt »Microsoft's role in fostering innovation« diesbezüglich doch etwas vage geblieben ist. [40]

[7] Es handelt sich auch keineswegs nur um Phänomene der ›ursprünglichen Akkumulation‹. Erst letztes Jahr ist Microsoft France vom Tribunal de Commerce in Nanterre wegen Code-Diebstahl – mit Microsofts Lieblingswort: »software piracy« – zu 3 Millionen Francs Geldstrafe verurteilt worden. [6]

›Was will er denn (schon wieder) von mir?‹ ist tatsächlich eine Frage, die Benutzer sich in Situationen stellen müssen, in denen die Software eigenmächtig und bevormundend oder sogar gegen ihre Interessen agiert.[8] Gute Software läßt die Initiative dem Nutzer, der dann nicht überlegen muß, was von ihm erwartet wird, sondern was er mit den ihm zur Verfügung stehenden Mitteln machen möchte. Die Richtlinie läßt vermuten, daß bei Microsoft ein Bild des Computerbenutzers herumgeistert, das vollkommen an dessen Bedürfnissen vorbeigeht und dem wir Programme zu verdanken haben, bei denen Büroklammer-Agenten uns den letzten Nerv rauben.

Microsofts Vorstellung von Innovation reflektiert ihre Marketing-Strategie, beide sind auf Expansion ausgerichtet. »Microsoft has built a monopoly business by throwing features into their products and dealing with the problems later.« [105] Viele ihrer technischen Bereicherungen bestehen darin, ein (übernommenes) Konzept mit allerlei Zusatzfunktionen anzureichern (-> 4.), die von Kritikern oftmals eher als Gadgetry angesehen werden und allzuoft hohe Sicherheitsrisiken mit sich bringen (-> 3.). Und bei nicht wenigen dieser ›Innovationen‹ stellt sich wiederum die Frage, wem sie zu Nutzen sind. Ein Beispiel einer neuen Technologie, zu der niemand sonst bislang die Dreistigkeit aufbrachte, hört auf den sinnigen Namen »Smart Tags«. Diese Helferlein waren noch in den letzten Testversionen von Windows XP implementiert, wurden aber aufgrund von öffentlichen Protesten nicht in die ausgelieferte Version übernommen. Smart Tags sind Links auf von Microsoft ausgewählte Sites, die vom System automatisch in vom Internet Explorer angezeigte Webseiten eingefügt werden. Der Software-Gigant hat sich damit das Recht erfunden, beliebigen Inhalten aus dem Netz den ›letzten Schliff‹ zu verpassen, indem sie ohne Wissen oder Zustimmung der Autoren Links hinzufügen – ein Eingriff, der verständlicherweise viele Reaktionen wie die von Dave Winer provozierte: »I won't write for a Web where Microsoft inserts links into my writing. ... what you're reading now is *my* document. I did not and will not give Microsoft the right to modify it.« [122] Microsoft verstand die Aufregung gar nicht, weil jeder Autor das Feature doch durch Einfügen einer (für den Leser unsichtbaren) Meta-Information in die Webseite verhindern könne. Ein solches pervertiertes Konzept der aktiven Deaktivierung (»opt-out«) ist dem üblichen Schwindel bei Spam-Mails vergleichbar, die dem Empfänger scheinheilig die Möglichkeit des »unsubscribe« anbieten.[9]

Eher berüchtigt ist Microsoft für ›Innovationen‹, die dem Ausbau und der Erhaltung seiner Marktbeherrschung dienen. Diese beinhalten Bundling-Strategien, um die

[8] Die zweite Frage – wo's denn nun lang geht – scheint eine recht eigenwillige Interpretation der Entwicklungsabteilung von Microsofts Werbeslogan »Where do you want to go today?« zu sein.

[9] Wir sind bereit zu wetten, daß Smart Tags eine Auferstehung erleben werden, vermutlich als Technologie, die von Webseiten und/oder Browsern explizit zugelassen werden muß (»opt-in«) und gegebenenfalls irgendeine Belohnung verspricht.

Nutzer stärker an die Interessen der Firma zu binden (-> 2.1, 2.3), penetrante ›Innovasionen‹ in die Privatsphäre der Nutzer, um diese besser kontrollieren und ›betreuen‹ zu können (-> 6.) und Taktiken des »embrace and extend«, bei denen freie Produkte oder Standards übernommen und so modifiziert werden, daß die ursprünglichen Konzepte und Entwicklungen, die sich daran halten, nicht mehr mit dem proprietären Massenartikel verträglich sind (-> 2.2). Wenn also Microsoft behauptet, die Bedürfnisse ihrer Kunden in den Mittelpunkt ihrer Überlegungen zu stellen [73], dürfte dies eine Projektion sein. Natürlich können zwischen den Interessen eines jeden Softwareherstellers und denen der Nutzer immer unauflösbare Widersprüche bestehen, bei einem Monopolkonzern ist dies aber zwangsläufig der Fall, weil Marktbeherrschung nicht im Sinne der Vielfalt von Nutzerinteressen sein kann.

2. Wie kann Microsoft mit technischen Mitteln andere Entwickler behindern oder gar ausschließen?

Microsoft kann sein Monopol bei Betriebssystemen dazu benutzen, auch in Bereichen der Anwendungssoftware eine Vormachtstellung zu gewinnen[10] – im Juristenjargon »monopoly leveraging« genannt – oder zumindest Einfluß darauf zu nehmen, welche Applikationen dem Nutzer ›zuhanden‹ sind und welche nicht. Die Tricks, mit denen eigene oder ›befreundete‹ Programme gefördert und unliebsamen anderen die Integration erschwert wird, sind oft nur Marginalien im großen Betriebssytemverbund. Sie nutzen die Unkenntnis oder das Desinteresse der meisten Nutzer an technischen Details aus, und ihr Sinn besteht ausschließlich darin, diesen die Wahl zwischen dem gut eingebundenen Produkt und der unzugänglichen Konkurrenz zu ›erleichtern‹. Innerhalb der Strategie, das Desktop-Monopol dazu zu nutzen, andere Entwickler zu behindern oder auszuschließen, lassen sich verschiedene Taktiken unterscheiden, die wir durch Beispiele illustrieren wollen:

1. durch Voreinstellungen eigene Programme bevorzugen und fremde benachteiligen;
2. durch Modifikation von offenen Standards andere Entwickler und Nutzer durch Inkompatibilitäten zur Verzweiflung bringen – »embrace and extend«;
3. durch Einschränken des Lieferumfangs unliebsame Anbieter behindern.

2.1 Registered File Types

In Windows wird der Typ einer Datei durch eine dreibuchstabige »Extension« bestimmt, die nach einem Punkt an den Dateinamen angehängt wird - ein Relikt des

[10] Dies ist Microsoft bekanntlich bei Spreadsheets und Präsentations-Software gelungen (-> 1.).

alten DOS-Systems. Die Zuordnung, welches Programm für welchen Dateityp zuständig ist und aktiviert wird, wenn man eine solche Datei öffnet, nimmt das Betriebssystem vor. Für manche Datei-Typen ist diese Information ›fest verdrahtet‹: *.exe*-Dateien sind ausführbare Programme, die das Betriebssystem startet; andere Datei-Typen sind anwendungsspezifisch: *.doc* etwa ist für Dateien reserviert, die von Microsoft Word erzeugt wurden. Schließlich gibt es eine ganze Reihe von Extensions, die im Prinzip an keine bestimmte Software gebunden sind, sondern nur bestimmte Datenformate anzeigen: *.gif* und *.jpg* etwa sind die vorherrschenden Bildformate im Web, *.mp3* das meistgenutzte Musikformat im Internet.[11]

Die Information, welche Anwendung für welchen Dateityp zuständig ist, ist in einer Tabelle der ›Registered File Types‹ abgelegt. Die Freiheit der Nutzer, selbst bestimmen zu können, welches Programm beispielsweise *mp3*-Dateien abspielt, hängt an der Frage, wie einfach der Eintrag in dieser Tabelle verändert werden kann. Die Hoheit über die »Registered File Types« stellt ein probates Mittel dar, die Vormachtstellung von Microsoft-Produkten in den Bereichen, in denen sie eigene Lösungen anbieten, abzusichern. »Microsoft protects its monopoly through a host of practices that barely register in the media or the public mind. The trial court's voluminous "findings of fact" only scratched the surface of the variety of stratagems the company employs to lock out competitors.« [100] Eine *mp3*-Datei wird beispielsweise standardmäßig vom Windows Media Player geöffnet und abgespielt, weil diese Belegung vom Betriebssystem vorgegeben ist. Der recht unübersichtliche Vorgang, diese Einstellung zu verändern, bleibt vielen Nutzern unklar, wodurch mp3-Player-Software von Drittanbietern mehr oder weniger effektiv vom Markt ausgeschlossen wird.[12] Folgt man der Argumentation von Scott Rosenberg, so repräsentiert die Art, wie das Ändern von Voreinstellungen realisiert ist, in subtiler Weise genau die unlauteren Geschäftspraktiken, deren Microsoft auch im Revisionsurteil für schuldig befunden wurde: »the problem with Windows' "registered file types" is just the sort of subtle but nasty Microsoft practice that many of us hoped a forceful antitrust ruling and tough remedy would finally change. It is one little example of the myriad techniques our most powerful operating-system vendor has at its disposal to screw competitors, take over new markets and -- contrary to its propaganda -- make users' lives more miserable.« [100]

---

[11] Eigentlich zeigt auch *.doc* nur eine bestimmte Text- und Layoutformatierung an. Da diese von Microsoft aber geheimgehalten wird, können Programme von anderen Herstellern nicht sehr gut damit umgehen. Ohne die sich daraus ergebenden Unverträglichkeiten würden viele Nutzer sicher bessere Textverarbeitungsprogramme verwenden.

[12] Die Möglichkeit, daß Applikationen bei der Installation zum Standard erklärt werden können, verlagert das Problem nur und erhöht nicht die flexible Entscheidungsgewalt der Nutzer. »Again, this takes choice out of the hands of users and puts us all at the mercy of developers who are trying to grab market share for their programs. Microsoft isn't the only troublemaker here. ... What Windows needs is a plain-English set of choices, in plain view, one that any novice user can easily find and understand, to tell the computer which program to use to open different kinds of files.« [100]

Die ›Lebensqualität‹ der durch ›Registered File Types‹ und ähnliche Mechanismen gegängelten Nutzer wird von Tom Regan in seinem Windows XP Review so beschrieben: »More than anything else, XP reminds me of a tourist trap. You arrive in a foreign city, and a handsome stranger walks up to you and says he will show you around the city. He offers to take you to the very best shops and restaurants. But you soon realize that he is taking you only to places that are owned by his relatives or by someone who gives him a kickback.« »Microsoft wants to make it as difficult as possible for you to exercise your own choice in what programs you want to use and where you get to go when you're online.« [95] Eine bemerkenswerte Charakterisierung des Erzeugnisses einer Firma, deren Slogan »Where do you want to go today?« lautet.

2.2 »Embrace and Extend«

Um seine Monopolstellung bei Betriebsystemen und ökonomisch interessanten Anwendungsprogrammen zu halten, muß Microsoft verhindern, daß eine kritische Masse an plattformunabhängigen oder -fremden Endnutzer-Anwendungen entsteht. Dazu dient die in der Vergangenheit mit großem Erfolg praktizierte Strategie ›embrace and extend‹, mit der durch proprietäre Abwandlungen von offenen Standards für andere Entwicklungen Unverträglichkeiten erzeugt werden. »To prevent pools of non-Microsoft applications from forming, Microsoft likes to appropriate what it calls "commodity protocols" (off-the-shelf, public protocols such as HTML, JavaScript, CSS and many more), and add proprietary extensions that prevent the formation of competing application pools.« [87]

Besonders ärgerliche Fälle dieser Praxis, proprietäre – euphemistisch »standards-based« genannte – ›Alternativen‹ in Umlauf zu bringen, waren in der Vergangenheit: Modifikationen des Sicherheitsprotokolls Kerberos, der plattformunabhängigen Programmiersprache Java und des HTML-Formats. Ein aktuelles Beispiel ist Microsofts Vorschlag eines »Soft Wi-Fi«-Netzes [116] [13], an dem sich in statu nascendi beobachten läßt, wie die Strategie funktioniert: Man nehme einen (meist) offenen Standard – hier ›802.11‹, ein von IEEE unter Mitwirkung von Firmen definierter Kommunikations-Standard für lokale drahtlose Computernetzwerke[14] – und integriere ihn in das eigene Betriebssystem oder auch in eine andere Software, die den Markt beherrscht: ›embrace‹. Dabei wird der Standard geringfügig modifiziert, möglichst ohne dies mit der den Standard erhaltenden Organisation zu koordinieren: ›extend‹. Es genügen einige unwesentliche Änderungen, mehr oder weniger bedeutungslose

[13] ›Wi-Fi‹ steht fürWireless Fidelity und bezeichnet Funknetzwerke, die dem Standard 802.11 folgen.

[14] Der Standard basiert auf einem Frequenzbereich, der für die unangemeldete und kostenlose Nutzung (nahezu) weltweit freigegeben wurde. Etliche Firmen bieten Geräte und Geräteteile für diese Art von drahtlosen Netzen an, und ein Firmenkonsortium stellt sicher, daß die Systeme untereinander kompatibel sind.

Verbesserungen oder Erweiterungen. Im Falle von Wi-Fi schlägt Microsoft das sogenannte »Soft-Wi-Fi« vor, bei dem Teile des Protokolls aus der Basisstation, die zwar nur einmal angeschafft werden muß, aber relativ teuer ist, in die Software des Betriebssystems verlagert wird. Solche weniger komplexen Basisstationen wären billiger, meint Microsoft, was dem Konsumenten und der Verbreitung von drahtlosen Netzwerken zugute käme.

Diese erleichterten Geräte funktionieren natürlich nur mit Microsoft Windows, weil Software in anderen Betriebssystemen wie Linux oder Mac OS sich an den 802.11-Standard hält, der mit »Soft-Wi-Fi«-Netzen aber nicht funktioniert. Die Marktmacht von Windows wird vermutlich dafür sorgen, daß sich die »Soft-WiFi«-Geräte durchsetzen werden, und wird folglich für die Nutzer aller anderen Betriebssysteme Probleme beim Einstieg in »Soft-Wi-Fi«-Netze schaffen, die von Konfigurations-Schwierigkeiten bis zum Ausschluß reichen können. Oder die anderen Entwickler passen sich (nicht zum erstenmal) Microsofts Vorgaben an. Bei einem proprietären Standard, den der Inhaber jederzeit ändern oder mit Beschränkungen belegen kann, kann dies aber dazu führen, wie der Hase hinter dem Igel herrennen zu müssen.[15] Natürlich kann ein solches Vorgehen des »de-commoditizing open standards into monopolistic lock-in devices« [91] nur dann funktionieren, wenn eine Firma in einem Bereich marktbeherrschend ist. Es wird im »Findings of Fact«-Dokument als eine der Methoden angeführt, mit der Microsoft seine Monopolstellung mißbraucht. [52]

2.3 Kontrolle der ausgelieferten Funktionalität

Ein direkteres Mittel zum Erhalt und Ausbau der Marktbeherrschung ist die Kontrolle des Lieferumfangs des Betriebssystems. Microsoft liefert zusammen mit Windows Software-Komponenten vieler anderer Hersteller aus. So befindet sich beispielsweise Treibersoftware[16] für Grafik- und Soundkarten verschiedenster Hersteller auf einer Windows Installations-CD oder auf einem vorinstallierten Rechner. Die Installation einer nicht mit Windows ausgelieferten Komponente stellt eine Hürde für viele Nutzer dar, sei es, daß sie aus dem Internet geladen werden muß oder auf einem Datenträger mit der Hardware ausgeliefert wird. Diese Situation verschärft sich noch, wenn eine Software lediglich neue Dienste und Funktionalitäten anbietet, beispielsweise Multimedia-Programme, Plug-Ins für den Browser und Ähnliches. Da der Betriebssytem-Monopolist exklusiv entscheiden kann, was er in seine Installation integriert, kann er nicht

[15] Die Modifikationen des Kerberos-Protokolls wurden von Microsoft zuerst überhaupt nicht offen gelegt. Nach einer massiven Kritik, konnte man die Abweichungen einsehen, mußte dazu aber in einer Lizenzvereinbarung unterschreiben, die proprietäre Spezifikation nicht ohne Microsofts Zustimmung zu veröffentlichen. [27]

[16] Treiber-Programme ermöglichen die Verbindung externer Hardware-Komponenten wie Drucker oder digitale Kameras mit dem Betriebssystem.

genehme Hersteller und Technologien einfach ausschließen und mit den ›Verbündeten‹ (für sich) vorteilhafte Verträge abschließen. So hat Microsoft zum Beispiel Rechnerhersteller, die ihre Geräte mit Windows 95 vorinstalliert verkaufen wollten, gezwungen, den Internet Explorer mit zu übernehmen, was ihnen 1995 durch ein Gerichtsurteil verboten wurde, aber zwei Jahre später vom Department of Justice immer noch eingeklagt wurde. [22] In den letzten Jahren lassen sich verschiedene Beispiele angeben, wie Microsoft die Kontrolle über den Lieferumfang dazu einsetzt, den Zugang für unliebsame Softwarehersteller oder konkurrierende Technologien zu erschweren. Dazu gehören unter anderem

– die im »Findings of Fact«-Dokument [52] von Richter Jackson festgehaltene Verdrängung von Netscape aus Windows;

– die Entwertung von Java durch den Entschluß, mit Windows XP keine eigene Runtime-Engine[17] für Java auszuliefern,– eine buchstäblich-smarte Auslegung der gerichtlichen Verurteilung ihrer früheren »embrace and extend«-Praxis, den Java-Standard durch Modifikationen zu unterlaufen. Die Firma, die sonst jedes Feature einbaut und aktiviert, meint diesmal, daß es sich bei Java um »a lot of code that many users don't need« handele und ihr Schachzug zu keiner Beeinträchtigung führe. [84] Tatsächlich sind Java-Applikationen und -Applets für Windows XP-Nutzer nur dann zu verwenden, wenn sie eine Java-Runtime downloaden (im Falle der verbreiteten Version von Sun rund 12 MB) und installieren – eine beträchtliche Hürde für normale Benutzer.

– die Einführung von signierten Treibern mit Windows XP. Microsoft bestätigt mit der Signatur die Eignung eines Treibers für Windows XP. Dieser Mechanismus kann die Stabilität des Betriebssystems verbessern, birgt aber auch die Gefahr eines monopolistischen Mißbrauchs. Dies hat Kodak Microsoft schon vor Auslieferung der ersten Windows XP Version vorgeworfen: Microsoft verweigere die Signatur für die Treibersoftware für digitale Kameras von Kodak offenbar, weil beide Firmen als Anbieter Web-basierter Dienste im Bereich der Digitalfotografie Konkurrenten sind.[18] [2] Nutzer finden sich künftig vor die Alternative gestellt, sich beim Installieren eines nicht-signierten Programms standhaft gegen eine Warnung des Betriebssystems vor einer »nicht getesteten« Software, die »vielleicht nicht zuverlässig ist« [2], zu behaupten oder doch lieber die von Microsoft empfohlene Software zu benutzen.

---

[17] In Java geschriebene Programme sind plattformunabhängig und brauchen daher zum Ausführen auf jedem Betriebssytem eine eigene Ausführungs-Software – die sogenannte Runtime-Engine.

[18] Eine verwandte Taktik besteht darin, Konkurrenten bei der Entwicklung von Schnittstellen zum Betriebssystem zu behindern. Ein Vertreter der Firma Palm hat im Microsoft-Prozeß ausgesagt, daß Microsoft die Interoperabilität von Palm PDAs mit Windows erschwere, indem sie Palm den Zugang zu geeigneten Entwicklungs-Tools verweigern. [55] Der Grund ist wohl ebenfalls darin zu sehen, daß Microsoft sich selbst im Bereich der PDAs engagiert. Im »Findings of fact«-Dokument ist festgehalten, daß diese Taktik ebenso gegen Netscape verwendet wurde.

Im ganzen Multimedia-Bereich kann man beobachten, wie Exklusionstaktiken zusammenspielen. Der mit Windows XP ›verbundelte‹ Windows Media Player 8 ist für das Abspielen von *.mp3*-Dateien voreingestellt; er kann diese (z.B. beim Überspielen von CDs) aber nicht erzeugen, der Nutzer wird hierfür auf (kostenpflichtige) Software von Drittanbietern verwiesen.[19] Der Media Player ›rippt‹ nur das proprietäre Windows Media Audio Format (WMA), was man als Versuch auffassen könnte, den populären mp3-Standard durch das eigene Musikformat zu verdrängen. Desgleichen würde Microsoft gern den offenen Videostandard MPEG-4 durch das ›abgewandelte‹ Windows Media Video Format (WMV) ›ersetzen‹. [20] Die Bestrebungen laufen darauf hinaus, das proprietäre Windows Media Format, zusammen mit der integrierten Digital Rights Management Technologie (DRM; -> 9.), als das »universelle Multimediaformat der Zukunft zu etablieren«. [98] Gegen Microsofts Monopolstrategien regt sich allerdings inzwischen auch außerhalb der USA politischer Widerstand. So überlegt die EU-Wettbewerbskommission zu verlangen, daß der Windows Media Player vom Betriebssytem entkoppelt wird, worauf prompt aus dem ›konvertierten‹ amerikanischen Department of Justice transatlantische Konflikte in Aussicht gestellt wurden, weil »monopoly leveraging« in den USA nicht als Vergehen angesehen werde. [62]

3. Was ist von Microsofts Sicherheitsinitiative zu halten?

In einem internen Memo vom 15. Januar 2002 fordert Bill Gates von seinen Mitarbeitern: »We must lead the industry to a whole new level of Trustworthiness in computing.« Er resümiert die bisherige Microsoft-Praxis und gibt vor, was sich daran ändern soll: »In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid email borne viruses.« [41]

Wenn eine simple, von Sicherheitsexperten schon lange angemahnte Modifikation von Outlook, die verhindert, daß Viren sich so leicht wie früher vermehren können, ein Beispiel dafür sein soll, was in Zukunft zu erwarten ist, erscheinen Zweifel an der

---

[19] In einer Beta-Version war es noch möglich, mp3-Dateien aufzunehmen, allerdings nur in schlechtester Qualität, was der Überzeugung, Microsoft wolle mp3 diskreditieren, Vorschub geleistet hat. [117]

[20] Hierbei finden sie in den Patenthaltern von MPEG-4 (unfreiwillige) Mitspieler, insofern als die auf Lizenz- und Nutzungsgebühren bestehen, was dazu geführt hat, daß Apple die neue QuickTime 6 Software zurückhält.

Folgenschwere der Kampagne angebracht.[21] Auch wenn die neue Initiative zu Schulungen, Crash-Kursen und einigen Tools geführt hat, überwiegt bei vielen Sicherheitsfachleuten die Einschätzung: »"too little, too late" or "we'll see how well it happens ... if it happens"«. [33] Um ernst genommen zu werden, wären massive Eingriffe in alle Microsoft-Produkte erforderlich. Die Sicherheitsexperten Bruce Schneier und Adam Shostack sowie Richard Smith haben wenige Tage nach Gates Proklamation Aufstellungen mit notwendigen konzeptionellen Änderungen vorgelegt [104], [112]; aber wohl die meisten unabhängigen Fachleute bezweifeln, daß der Monopolist, so wie man ihn kennt, dazu willens und in der Lage ist. Steve Ballmers ›Selbstkritik‹: »I think the core code is OK. It's not like the core design is bad.« dürfte ein Indiz für die Berechtigung des Zweifels sein. [20]

Das Jahr 2001 verzeichnete eine enorme Verbreitung an Viren-Attacken, deren Grundlage überwiegend Sicherheitsschwachstellen von Microsoft waren. Außerdem ist (nicht nur in den USA) nach dem 11. September eine Sicherheitshysterie entstanden, die in einem Klima des Patriotismus gedeiht. Deshalb glauben Fachleute wie Richard Forno: »... Microsoft Security Day is the software giant's latest attempt to cheaply use public policy concerns as propaganda for product marketing while hopefully currying some patriotic mindshare along the way from both the government and consumers.« [33] Microsofts Michael Lane Thomas nutzte die Gelegenheit, »industrial terrorists [who] analyzed IIS Web server security until they found a weakness« mit den Terroristen vom 11. September zu vergleichen, und er appellierte an patriotische Gefühle, als er unabhängige Analysten wie die Gartner Group schalt, weil deren Empfehlung, von Microsofts unsicheren Servern auf andere Produkte umzusteigen, »would only accomplish what the industrial terrorists want.« [63]

Vertrauenheischende Propaganda ist notwendig geworden, weil Sicherheitsprobleme von Microsoft-Produkten letztes Jahr fast wöchentlich in den Medien waren und der Erfolg der .NET-Initiative davon abhängen wird, das Vertrauen der Konsumenten, vor allem aber der potentiellen Anbieter von Web-Diensten und -Inhalten zu gewinnen.[22] »The simple truth is that Microsoft has a serious image problem when it comes to the reliability, security, and stability of its network services and products.« [33]

---

[21] »If this is Gates' idea of a security job well done, then all we have here is another PR smokescreen.« [46] Es gibt auch Sicherheitsfachleute, wie Allan Paller vom SANS Institute, die meinen, die Initiative könnte einfach als gute Ausrede bei Terminschwierigkeiten dienen: »I bet every delayed product this year will be due to security concerns«. [57]

[22] In den Product Use Rights (PUR) muß der Nutzer von Windows XP Microsoft das Recht einräumen, »security updates« auf seinem Rechner zu installieren. Allerdings handelt es sich dabei um neue Versionen des Digital Rights Management Systems (DRM; -> 9.), »that a secure content owner has requested that MS, Microsoft Corporation, or their subsidiaries distribute«. Ed Foster meint dazu: »In other words, it would seem Microsoft's idea of a security update is one that protects the property rights of vendors, not the security of customers' systems.« [35]

Es würde ein eigenes Buch füllen, die unrühmliche Geschichte der Sicherheitsprobleme bei Microsoft-Software zu schreiben. Wir beschränken uns hier auf einige ›sensationelle‹ Aspekte von Malware (»malicious software«), die in den letzten Jahren Schlagzeilen gemacht haben.[23]

Virus[24]	Auftreten	Schaden[25]	Art
Melissa	1999	1100	Word Macro-Virus
I Love You	2000	8750	Email-Virus/Wurm
SirCam	2001	1150	Email-Virus/Wurm
Code Red I, II	2001	2620	Würmer
Nimda	2001	635	Wurm

Melissa war ein Makro-Virus, der sich in Word-Dokumenten verbreitete. Das Öffnen eines infizierten Dokumentes aktivierte den als Makro ›getarnten‹ Virus, der sich nun mit diesem Dokument per Email als Attachment an 50 Adressen aus dem Adreßbuch des infizierten Rechners verschickte. Die Tatsache, daß ein Script[26] aus Word heraus Emails ohne Wissen und Zustimmung des Nutzers verschicken konnte, ist als grobe Sicherheits-Lücke von Word und des Scripting-Mechanismus anzusehen.

Der »I Love You«-Virus breitete sich (unter anderem) ebenfalls durch Email-Attachments aus, deren Script-Code in Outlook durch Anklicken aktiviert wurde, Dateien auf dem befallenen Rechner zerstörte und sich per Outlook an Adressen aus dem Adreßbuch verschickte. »I Love You« verbreitete sich sehr schnell, so daß Viren-Scanner nutzlos waren, und verursachte bislang den größten geschätzten Schaden. Die Tatsache, daß in einem Email-Programm Script-Code mit einer Vielzahl von potentiell zerstörerischen Aktionen ausgeführt werden kann, ist eine grobe konzeptionelle Sicherheitsschwäche von Outlook und dem implementierten Scripting-System.[27] Hier

---

[23] Eine detaillierte Beschreibung der ›eindrucksvollsten‹ Viren und Würmer findet sich in [25].

[24] Es ist üblich geworden, verschiedene Arten von Malware übergreifend als Viren zu bezeichnen. Streng genommen brauchen Viren einen Wirt, mit dem sie zusammen ausgeführt werden, während Würmer selbständig agieren.

[25] Schadensschätzung laut einer Studie von Computer Economics in Millionen US $. (Stand Ende 2001) [13]
Zahlenangaben über Schäden durch Malware sind mit größter Vorsicht zu genießen, weil Hersteller von Viren-Scannern ein Interesse daran haben zu übertreiben, die geschädigten Organisationen hingegen zu untertreiben. Die Höhe des verursachten Schadens sagt auch wenig über die Potenz eines Virus aus. Die raffiniertesten Spezies aus obiger Liste waren keineswegs die bösartigsten. Und schließlich ist zu beachten, daß Schäden, die durch Insider oder durch schlicht fehlerhafte Programme verursacht werden, um ein Vielfaches größer sind.

[26] Scripte sind simple, spezialisierte Programme in Klartext, die bei der Ausführung übersetzt werden.

[27] Wenn Microsoft in der »General Information About Using VBScript with Outlook« behauptet(e): »VBScript is designed to be a secure programming environment. It lacks various commands that can be potentially damaging if used in a malicious manner. This added security is critical in enterprise solutions.« , dann kann man das wohl nur dahingehend interpretieren, daß es noch viel Schlimmer hätte kommen können. [78] Steven Vaughan-Nichols hält dagegen: »Outlook is vulnerable by design.« ; und er empfiehlt: »disable all options for ActiveX Controls and plugins and Scripting«, oder noch konsequenter: »Ban Outlook – now«. [120]

trifft der bekannte Ausdruck informatischer Naivität einmal mehr ins Schwarze: »It's a feature, not a bug.«

Auch der SirCam Wurm verbreitete sich dank der Sicherheitsschwachstellen mittels Windows Adreßbuch und versteckte sich dabei in attachten Dokumenten, die auf dem infizierten Rechner zufällig ausgewählt wurden. Hier kam also unter Umständen der Schaden einer massiven Verletzung der Privatsphäre hinzu.

Der Code Red Wurm trat in verschiedenen Varianten auf und infizierte in kurzer Zeit mindestens 350000 Microsoft Internet Information Server (IIS). Er nutzte einen kurz zuvor publizierten Programmierfehler des IIS-Servers aus, der zu einem Buffer Overflow führt.[28] Die erste Version versuchte außerdem eine »Denial of Service«-Attacke auf den Server des Weißen Hauses (-> 4.2), die jedoch durch eine ungeschickte Implementierung scheiterte; der eigenständige Nachfolger Code Red II installierte zusätzlich eine ›Backdoor‹ auf den befallenen Servern, die einen späteren ›remote‹ Zugang ermöglichte. [39]

Nimda war der bislang komplexeste Wurm, der gleich mehrere Sicherheitslücken von Microsoft-Produkten ausnutzte und sich auf ganz verschiedene Weisen ausbreitete: Unter anderem überprüfte er, ob die von Code Red II hinterlassene Backdoor noch existiert und verbreitete sich als Attachment einer HTML-Email mit einem MIME-Typ[29], der von Outlook und Outlook Express ausgeführt wurde, ohne daß man das Attachment öffnete; es reichte, daß man die Email las oder im Previewer anschaute. Dank einer mangelhaften Überprüfung der mehrere Bytes langen Zeichendarstellung im Unicode konnte Nimda auch auf direktem Wege im IIS-Server ausgeführt werden, und er fügte Web-Seiten auf den befallenen Servern eine JavaScript-Zeile hinzu, die bewirkte, daß man sich mit dem Wurm infizierte, wenn man eine solche Seite mit dem Internet Explorer lud, weil der den Wurm-Code brav ausführte.[30] [64]

---

[28] Bei einem Angriff, der auf einem Buffer Overflow beruht, werden in ein fehlerhaftes Programm längere Werte eingegeben, als dafür Speicherplatz vorgesehen ist. Dadurch gerät das Programm bei seiner normalen Abarbeitung in einen falschen Bereich und kann auf ein vom Angreifer geschriebenes Programmstück gelenkt werden, das irgendwelche Bosheiten ausführt. Buffer Overflows sind die ältesten und weitaus häufigsten Ursachen für Sicherheitslücken; sie sind immer das Ergebnis schlampiger Programmierung, denn es werden Bereichsgrenzen nicht abgefragt. Solche ›Kleinigkeiten‹ können große Wirkungen haben. So ist es z.B. möglich, sich einen Virus einzufangen, wenn man die lästigen digitalen ›Visitenkarten‹ (vcf-Attachments bei Emails) in Outlook oder Outlook Express öffnet, weil dort beim Geburtsdatum ein Buffer Overflow erzeugt werden kann. [48]

[29] MIME-Types (».Multipurpose Internet Mail Extensions«) geben bei Übertragungen von Dateien im Netz an, um welchen Dateityp es sich handelt. Nimda tarnte sich mit dem MIME-Type *audio/x-wav* für Musikstücke, aber statt automatisch ein Ständchen abzuspielen, wurde der Wurm-Code ausgeführt. Schuld hieran war ein Bug des Internet Explorers, der von Outlook bei HTML-Mails benutzt wird.

[30] Sicherheitslücken des Internet Explorers (IE) würden in dem hypothetischen Schwachstellenbuch mehrere Kapitel füllen. Georgi Guninski, der viele IE-Fehler entdeckt hat, empfiehlt in der »Security Advisory # 52« als vorbeugende Maßnahmen: »Disable Active Scripting and never turn it on. Better, do not use IE in hostile environments such as the internet.« [47]

Windows XP wurde als das bisher sicherste Betriebssystem von Microsoft angekündigt; in einem Interview verkündete Vizepräsident Jim Allchin stolz: »Windows XP is dramatically more secure than Windows 2000 or any of the prior systems. ... We have gone through all code and, in an automated way, found places where there could be buffer overflow, and those have been removed in Windows XP. We have also turned off by default a whole set of things so that users are configured in a minimalist kind of way, making them less vulnerable. «. [28] Kurz darauf wurde ein Buffer Overflow in dem automatisch aktivierten Feature »Universal Plug and Play« (UPnP) entdeckt, der es einem Cracker[31] erlaubt, jeden XP-Rechner, der online ist, vollständig zu kontrollieren. Microsofts Sicherheitsmanager Scott Culp erkannte zwar an, daß eine »very serious vulnerability« mit dringendem Handlungsbedarf vorliege: »Every Windows XP user needs to immediately take action.«, aber zugleich verstieg er sich zu der grotesken Behauptung: »This is the first network-based, remote compromise that I'm aware of for Windows desktop systems«. [8]

Natürlich stellt Microsoft nach der Veröffentlichung einer Sicherheitslücke oder nach einem Viren-Desaster Security Patches[32] auf ihren Servern zur Verfügung, – im Falle von Code Red war der Patch tatsächlich schon verfügbar, bevor der Wurm sein Unwesen trieb. Aber sehr viele Nutzer bekommen dies nicht mit, wissen nichts damit anzufangen oder finden Nachsorge nicht so wichtig, und so bleiben viele Rechner mit ungepatchter Software weiterhin verletzlich, – auch für die Viren, von denen wir oben leichtsinnig in der Vergangenheit gesprochen haben. (Tatsächlich ist SirCam noch immer höchst aktiv.) Allerdings kann man als Nutzer oder Administrator auch schnell den Anschluß verlieren, denn Microsoft hat in den Jahren 1999, 2000 und 2001 immerhin ca. 60, 100 und 60 Security Bulletins veröffentlicht und dementsprechend viele Security Patches ausgeliefert. [72] Es ist also nicht verwunderlich, wenn Richard Forno von einem »decades-old proprietary patchwork of many Microsoft products« spricht und den durchschlagenden Erfolg der Sicherheitsinitiative etwas schief sieht: »Undoubtably, history will remember January 16, 2002 as Microsoft Security Day – harkening back to that wonderous day in 1995 when Chairman Gates announced that the Internet was to be part of all Microsoft products and services. That proclaimation produced such well-known Redmond innovations as Melissa, I Love You, Code Red, SirCam, Code Red II, BadTrans, UPnP, and VBScript, among other notables, resulting in burned-out system administrators and a flourishing information security industry.« [33]

---

[31] Hacker sind, zumindest in ihrem Selbstverständnis, einfach nur gute Programmierer, Cracker dagegen sind Hacker, die Schaden verursachen wollen. Der Sprachgebrauch ist allerdings nicht einheitlich.

[32] Ein Patch ist ein Programmstück, das nachträglich installiert wird und ein fehlerhaftes Programmteil ersetzt.

4. Wieso gibt es denn bei Microsoftprodukten so viele Sicherheitsprobleme?

Betrachten wir nochmal Bill Gates Epistel: »In the past, we've made our software and services more compelling for users by *adding new features and functionality*, and by making our platform richly extensible. We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize *security right out of the box, ...* .« [41]

Darin haben wir zwei kritische Punkte hervorgehoben, die die Praxis von Microsoft kennzeichnen:

1. Microsoft-Software wird mit Voreinstellungen ausgeliefert, in denen fast jede Funktionalität und jedes Feature aktiviert ist. Das meiste davon benötigt der normale Nutzer nicht, ein Cracker kann es dafür umso mehr gebrauchen.[33]
2. Die Anhäufung von solchen Features macht einen Großteil von Microsofts Entwicklungen aus, weshalb boshafte Menschen hier von »bloatware« sprechen. Es geht darum, in der ›richly extensible platform‹ mehr Features zu haben als die Konkurrenz, gleich welche Sicherheitsrisiken das mit sich bringt.

Wir wollen mit zwei Beispielen andeuten, wie problematisch diese Praxis sein kann.

4.1 Verstecken der Datei-Extensions

Wie schon erwähnt, wird in Windows der Typ einer Datei durch eine dreibuchstabige Extension bestimmt und vom Betriebssytem entsprechend interpretiert (-> 2.1). *Gates.exe* ist ein ausführbares Programm, *Gates.doc* ein Word-Dokument und *Gates.jpg* ein Bild im standardisierten JPEG-Format. Extensions repräsentieren also Meta-Daten, Daten über die Daten.[34] Ab Windows 98 werden diese ›Anhängsel‹ aber vom Betriebssystem standardmäßig nicht mehr angezeigt. *Gates.exe*, *Gates.doc* und *Gates.jpg* heißen jetzt alle nur noch *Gates* und unterscheiden sich lediglich durch ihre Icons, die man aber auch ersetzen kann. Technisch versierte Nutzer können diese Voreinstellung ausschalten und die Extensions wieder anzeigen lassen (und tun dies

---

[33] In seiner Expertenbefragung über »The Twenty Most Critical Internet Security Vulnerabilities« führt das SANS Institute Default-Installationen an erster Stelle auf. [103] Auch das ›sicherste‹ Windows XP wird mit riskanten, standardmäßig aktivierten Features ausgeliefert, die wie UPnP zu Desastern führen können (-> 3.). Alles und jedes vorzuinstallieren, hat den angenehmen Nebeneffekt, Kunden-Support einzusparen, weil weniger Nutzer anrufen werden, die ein angekündigtes Feature nicht einsetzen können.

[34] Der elegantere und technisch überzeugendere Ansatz des Mac OS, Meta-Daten außerhalb der eigentlichen Daten zu speichern, führt dazu, daß die Information über den File-Typ beim Transfer auf ein Windows-System verloren geht, weil keine entsprechende Extension vorliegt. Um mit den allgegenwärtigen Windows-Systemen kompatibel zu sein, ist inzwischen das Mac OS dazu übergegangen, den File-Typ auch in einer Extension zu speichern und die eigenen Konzepte aufzugeben.

auch meist).[35] Wie bei vielen Voreinstellungen überfordern solche Änderungen einen Großteil der Nutzer. Auf den ersten Blick scheint das Feature der versteckten Extensions gerade für solche Nutzer Vorteile zu bringen. Der File-Typ muß etwa bei Namensänderungen nicht mehr berücksichtigt werden, und vor allem braucht der ›unbedarfte‹ Nutzer das Konzept der Extensions und Dateitypen nicht mehr zu verstehen. Jedoch öffnet diese voreingestellte Blindheit dem Mißbrauch Tür und Tor: Wenn man die Datei *Gates.exe*, deren Name nur als *Gates* angezeigt würde, in *Gates.mp3.exe* umbenennt, wird dem Nutzer tatsächlich *Gates.mp3* angezeigt, obwohl es sich bei der Datei um ein ausführbares Programm handelt. Die Möglichkeit dieses ›Schwindels‹ wurde von vielen Viren (z.B. »I Love You«) ausgenutzt, die über Email-Attachments solcherart getarnte *.exe*-Dateien versendeten und auf die technische Unwissenheit oder die Unaufmerksamkeit der Empfänger bauten. Obwohl dieses »out of the box«-Feature von Windows über Jahre hinweg beträchtlichen Schaden angerichtet hat, wurde keine befriedigende Lösung für die durch diese ›Innovation‹ verursachte Sicherheitsschwäche implementiert.

4.2 Zombies im Sonderangebot

Microsoft hat Windows 2000/XP um Funktionalitäten erweitert, die frühere Sicherheitsvorkehrungen aufgeben und es erlauben, Windows-Rechner einfacher für eine »Distributed Denial-of-Service« (DDoS) Attacke einzusetzen. [42] DDoS-Attacken stellen eine wachsende Bedrohung von Servern im Internet dar, wobei die Opfer nicht fahrlässig zu sein brauchen und sich kaum dagegen wehren können. Bei einer DDoS-Attacke wird ein Internet-Server mit so vielen unbeantwortbaren Anfragen bombardiert, daß er sie nicht mehr bewältigen kann.[36] Erfolgt ein solches Bombardement über längere Zeit, verschwindet der Server praktisch aus dem Netz, weil er (fast) keine echten Anfragen mehr beantworten kann. Der Angreifer benötigt dazu ›Verbündete‹, die alle gleichzeitig das Opfer attackieren (»Distributed DoS«). Solche ohne Wissen und Zustimmung ihrer Nutzer beteiligten ›Hilfsrechner‹ sind zuvor durch das Ausnützung von Sicherheitslücken ›gehackt‹ worden. Man nennt sie »Zombies«, weil sie von außen aktiviert und befehligt werden können.

---

[35] Microsoft listet 38 Extensions auf, deren Dateien zur Gefahr werden können. [77] Einige davon werden auch nach der Rückstellung des Versteck-Features weiterhin ohne Extensions angezeigt, was sich erst durch einige, nicht unproblematische Lösch-Operationen in der Windows Registry beheben läßt. [14]

[36] »Denial-of-Service« (DOS) Attacken nutzen folgenden Mechanismus aus: Bekommt ein Internet-Server eine Anfrage, die er nicht beantworten kann, weil sie etwa einen unbekannten (gefälschten) Absender hat, wartet er eine bestimmte Zeit (z.B. 20 Sekunden), bevor er die Anfrage entfernt. Ein Server kann natürlich nur eine bestimmte Menge von gleichzeitig eintreffenden Anfragen bearbeiten, deren Anzahl sich durch die zur Verfügung stehende Bandbreite und durch die Kapazitäten des Rechners mit der darauf laufenden Software bestimmt. Wenn nun gleichzeitig mehr unbeantwortbare Anfragen eintreffen, als der Server verarbeiten kann, so ist er während der Wartezeit für alle weiteren Anfragen ›taub‹; – er »verweigert seinen Dienst«.

Durch eine Neuimplementierung der Netzwerk-Schnittstelle wird Windows XP zu einem idealen Mitspieler in DDoS-Attacken. In Windows 9x/NT wurde der Netzwerk-Code am Zugriff auf den ›protokollarischen Kern‹ des Internets, sozusagen die allgewaltige Technik im Keller, gehindert. Dadurch waren diese Versionen für Cracker nur eingeschränkt verwendbar. Mit Windows 2000 wurde eine neue Netzwerk-Komponente implementiert, die über ein Feature namens »raw sockets« einen direkten Zugriff auf diese inneren, protokollarischen Ebenen des Internets erlaubt.[37] Für die Nutzung bringt das keine relevanten Vorteile, aber jede Menge neue Gefahren. Denn dadurch wird es möglich, den Absender von Datenpaketen zu fälschen (»IP-spoofing«), was eine wesentliche Voraussetzung für die beschriebene DDoS-Attacke darstellt und in der ›Szene‹ mit Wohlgefallen registriert worden ist. [42]

In Windows 2000 existiert noch einen gewisser Schutz, weil hier der für den Zugang zu »raw sockets« notwendige Status des Administrators ein privilegierter ist. In der Windows XP Home Edition, das eine »Consumer-Level Software« sein soll, kommt die zweite ›Enthemmung‹ hinzu, daß praktisch jeder Nutzer auch Administrator ist, falls man nicht ziemlich komplizierte Sicherheitsvorkehrungen trifft. [119] Diese riskante Rollenzuweisung bringt mit sich, daß nahezu jeder Prozeß mit ›root‹-Rechten laufen kann. Durch den Consumer Level von XP wird diese Lockerung doppelt gefährlich, weil solche Nutzer meist nicht technisch versiert sind und ihre Rechner nicht durch Patches und Abschottungsmaßnahmen vor der Übernahme als Zombie zu schützen wissen. Microsoft vertreibt die Windows XP Home Edition als das »sicherste Windows für Heimanwender aller Zeiten«, aber für das am 25. Oktober 2001 ausgelieferte XP-System sind bis Mitte Januar schon sechs Security Fixes nachgereicht worden [38], und durch die neuen Features wurde es zu einem begehrenswerten Ziel für Cracker gemacht. Man wird sehen, ob die neue Sicherheitsinitiative von Microsoft zumindest diese neue Schwachstelle behebt.

Während Bill Gates das »adding of new features« euphorisch als einen »terrific job« bezeichnet hat, sieht Phil Agre darin ein erschreckendes Phänomen der Unreife: »What really causes these endless computer security disasters? We've talked about economic factors, but now I think we have to talk about another factor: weenies.[38] Weenies come in two varieties, tech and marketing. ... The most distinctive feature of weenies is the worship of features. Tech weenies want everything to be cool: that means hyper-general, hyperprogrammable, hyperextensible, no matter what hazards might result. Marketing people obsessively look at the complete list of features in their competitors

[37] Dieses Feature ist in UNIX-basierten Betriebssystemen traditionell vorhanden, aber dort gibt es einen gewissen Schutz vor Mißbrauch, weil man nur mit den Rechten eines Superusers darauf Zugriff hat (»root-access«). Vermutlich hängt Microsofts ›Innovation‹ auch damit zusammen, daß sie Teile des Netzwerkcodes einem Open-Source Produkt (FreeBSD UNIX) entnommen haben, ohne das zugehörige Sicherheitsmodell zu übernehmen. [44]

[38] Als Angehörige der TU Wien würden wir die Übersetzung ›Würstl‹ der Denotation ›Wiener‹ vorziehen.

products and command the tech weenies to include all of them, and then to differentiate the product by adding more. ... Security catastrophies will not disappear until the weenies are all under adult supervision. This will never happen at Microsoft, which is managed by two-year-olds who hire people just like themselves. One more reason to shut it down.« [1]

5. Wie reagiert Microsoft auf publik gewordene Sicherheitsmängel?

Microsofts Politik im Umgang mit schlechter Presse und Kritik an ihren Sicherheitsmängeln läßt sich auf die Formeln bringen: ›blame the user‹, ›blame the administrator‹, ›blame the hacker‹; und ihre bevorzugte Sicherheitsstrategie dürfte ›security through obscurity‹ sein.

Nach der »I Love You«-Epidemie (-> 3.) erklärte der Microsoft-Sprecher Adam Sohn auf die Frage, wie Firmen sich vor solchen Katastrophen schützen könnten, im Scherz: »They should commence by beating their employees« [39], bestritt dann aber völlig im Ernst jede Verantwortung für das Desaster. Schuld seien die dummen Nutzer, die Attachments anklicken. »”People shouldn't open them", said Sohn. "That's the problem.”« [1] Eine damals von Microsoft veröffentlichte Virus-Warnung behauptete gar: »Customers can avoid being affected by this and other viruses by following standard best practices: ++ Never run an executable from someone you don't know. ++ Always have a good-quality virus scanner. ++ Always keep the virus scanner's signature files up to date.« [82] Nun ist es zwar richtig, daß viele User nach wie vor zu vertrauensselig mit Attachments umgehen, der Trick des Virus, sich über die Einträge im Adreßbuch des befallenen Rechners zu verbreiten, sorgte jedoch dafür, daß die infizierte Mail an Bekannte verschickt wurde und folglich nicht »from someone you don't know« kam.[40]

Die propagandistischen Bemühungen von Microsoft waren ganz darauf gerichtet, die direkte Verbindung zwischen dem »I Love You«-Virus und ihren Produkten zu vernebeln. So beginnt obige Warnung erstmal mit einer unsinnigen Verallgemeinerung: »Last week a new virus began circulating through e-mail that has the potential to affect a wide range of e-mail users including those users running Microsoft Outlook.« [82] Der evidente Zusammenhang zwischen der Ausbreitung des Virus und dem Outlook-Feature, Skripte unkontrolliert auszuführen, wird wegargumentiert: »The issue here isn't scripting. It's the social phenomenon of virus writing. That virus could have

[39] Pikanterweise waren auch viele von Microsofts Firmenrechnern befallen, und der Virus breitete sich auch aus dem Firmennetz heraus weiter aus.

[40] Der Disclaimer in der Virus-Warnung, den wir eingangs selbst verwendet haben, war bei dieser Informationspolitik offensichtlich zurecht angebracht.

been written as an executable or on any platform or in a nonscripting language. Just because this virus was written in a scripting language, and we happen to support scripting in our operating system, doesn't make it a security issue.« [30] Phil Agre, der die »slippery language Microsoft has used to evade responsibility for the security problems that were exploited by the most recent e-mail virus« unter rhetorischen Gesichtspunkten untersucht hat, bemerkt dazu: »Blaming "the social phenomenon of virus writing" is not reasonable. A product that can be subverted by a random college student to cause massive worldwide damage is not secure. That's what "secure" means.« [1] Microsofts Sicherheitsmanager Scott Culp hingegen machte gar die Popularität von Microsoft dafür verantwortlich und bestritt jede Sicherheitslücke: »In this case the virus author chose to target Outlook probably because it gave him better reach. There isn't a security vulnerability in Outlook involved in this at all.« [1] Knapp zwei Jahre später verkauft Bill Gates dann die Deaktivierung des inkriminierten Features als initialen Erfolg der neuen Sicherheitsinitiative: »A good example of this is the changes we made in Outlook to avoid email borne viruses.« [41]

Schuld haben auch die Administratoren, die nicht die bereitgestellten Security Patches installieren. Tatsächlich ist erstaunlich, wie gering viele Systemadministratoren, die eigentlich vom Fach sein sollten, Sicherheitsprobleme erachten. Beispielsweise wurde festgestellt, daß fast 40% der vom ersten Code Red Wurm befallenen IIS-Server bei der zweiten Attacke immer noch infizierbar waren, weil sie keinen Security Patch aufgespielt hatten. [39] Jedoch ist die Schuldzuweisung an die Administratoren auch ziemlich vermessen, wenn man bedenkt, daß Microsoft in den letzten Jahren so viele Security Patches nachgereicht hat, daß durchschnittlich ein bis zwei Updates pro Woche erforderlich waren. Hinzu kommt, daß nicht wenige Nutzer den IIS-Server in Windows 2000/NT installiert haben, ohne etwas damit zu machen, und unter Umständen gar nicht bemerken, daß sie gefährdet oder infiziert worden sind.

Peinlich für Microsoft ist die öffentliche Diskussion ihrer Sicherheitsprobleme.[41] Nach dem für ihr Image katastrophalen Jahr 2001 gehen ihre Bestrebungen nun dahin, das Veröffentlichen von Schwachstellen zu ächten. Scott Culp spricht von einer »information anarchy«, wenn Sicherheitsexperten entdeckte Fehler publik machen, weil dies Crackern erst ermöglichen würde, sie zum Schaden aller auszunutzen. Wie mit

[41] Den Grund dafür, daß Microsoft es sich erlauben kann, »security vulnerabilities as public relations problems« zu behandeln [105], sieht der Sicherheitsexperte Bruce Schneier in unseligen Mechanismen des Marktes begründet: »The upshot of this is that the marketplace doesn't reward real security. ... Microsoft knows that reliable software is not cost-effective. According to studies, 90 to 95 percent of all bugs are harmless. They're never discovered by users, and they don't affect performance. It's much cheaper to release buggy software and fix the 5 to 10 percent of bugs people find and complain about. Microsoft also knows that real security is not cost-effective. They get whacked with a new security vulnerability several times a week. They fix the ones they can, write misleading press releases about the ones they can't, and wait for the press fervor to die down (which it always does). And six months later, they issue the next software version with new features and all sorts of new insecurities, because users prefer cool features to security.« [106]

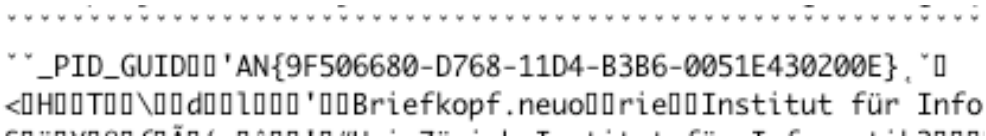
entdeckten Sicherheitslücken zu verfahren sei, wird kontrovers diskutiert, wobei sich zwei konträre Positionen auszeichnen lassen: »'security through obscurity,' in which it's hoped that concealing an exploitable defect will prevent exploitation, and 'full disclosure,' which works on the premise that forewarned is forearmed, and which most professionals now prefer.« [102] Das Geheimhalten von Sicherheitsschwächen bietet natürlich keinen Schutz, solange es Menschen gibt, die sie entdecken und (eventuell unbemerkt) ausnutzen. »Microsoft's security through obscurity will only give these guys an exclusive advantage, because they'll find and use the holes that no one is expecting to be found.« [102] Andererseits ist eine ›professionelle Hilfestellung‹ durch Veröffentlichung nicht unproblematisch, wie sich beim Code Red Wurm gezeigt hat, der vier Wochen nach der Veröffentlichung des Buffer Overflow Problems beim IIS-Server in Umlauf war. Zur Zeit werden Kompromißvorschläge diskutiert, die darauf hinauslaufen, Sicherheitslücken dem Hersteller zu melden und erst nach einer Schonfrist (z.B. von 30 Tagen) zu veröffentlichen [101], – eine Praxis, die sowieso schon weitgehend üblich ist. Zum zweischneidigen Verfahren des »full disclosure« ist es tatsächlich erst deshalb gekommen, weil sich in der Vergangenheit gezeigt hat, daß viele Hersteller – nicht zuletzt auch Microsoft – ohne den Druck der Öffentlichkeit garnicht oder nur langsam reagieren und Sicherheits-Patches lieber unauffällig mit dem nächsten ›normalen‹ Update ausliefern.

Schlechte Nachrichten schaden dem Image und dem Absatz der Hersteller. Noch vor Bill Gates Trustworthiness-Proklamation hat Scott Culp Pläne für ein Microsoft Security Framework vorgestellt, das Richard Forno als »yet another vendor-biased "club" to try and restrict the discussion of vulnerability information away from the public« charakterisiert. [32] Ein solches »Informationskartell« für Sicherheitsprobleme würde für Fachleute und engagierte Nutzer, die nicht dazu gehören, eine Bedrohung darstellen, nach dem Digital Millennium Copyright Act (DMCA) angeklagt zu werden (-> 9.), wenn sie Sicherheitslücken veröffentlichen. Die zunehmende Verquickung von Urheber-rechtsregelungen mit Sicherheitsaspekten fördert die bequemere Strategie des ›security through obscurity‹, denn es besteht wenig Anreiz, schlechte Software zu verbessern, wenn man potentielle ›Whistle Blower‹ durch drakonische Strafen abschrecken kann. In diesem Zusammenhang bekommt Microsofts Digital Rights Management Betriebssystem (DRM OS) eine zusätzliche Bedeutung (-> 9.). Denn ein tief im Betriebssytem verankerter Schutzmechanismus für urheberrechtlich geschütztes Material, würde es erlauben, jemanden, der eine Sicherheitslücke im Betriebssytem aufdeckt, auch deshalb zu verfolgen, weil die Veröffentlichung wahrscheinlich ermöglicht, den Rechteschutz zu umgehen. Auch ohne paranoid zu sein, gibt es zu denken, daß Microsoft Anfang des Jahres mit Scott Charney jemand zum Chief Security Strategist berufen hat, der kein Informatiker sondern Jurist ist und vorher Ankläger von Cybercrime-Vergehen war. [85]

6. Wie hält es Microsoft mit der Privatsphäre der Nutzer?

Mit Windows 98 führte Microsoft einen Service ein, mit dem man das Betriebssystem online beim Hersteller registrieren lassen konnte. Eine online-Registrierung war Voraussetzung dafür, später online Updates herunterladen zu dürfen. Die Registrations-Software schickte aber gleichzeitig einen Global Unique Identifier (GUID) des Rechners[42] an Microsoft. [68] Nach der Aufdeckung dieser heimlichen Datenübertragung beteuerte Microsoft schnell, daß man diese Information nicht auswerten oder verwenden würde; aber auch dann stellt die stille Post einen massiven Eingriff in die Privatsphäre der Kunden dar.

In Version 7 (Office 97) werden eindeutige Rechner- und Software-Identifikationen auch in die von Excel und Word erzeugten Dateien eingebettet. Dabei wird die Seriennummer (PID = Programm-ID), mit der die Software registriert ist, zusammen mit dem GUID in den Dokumenten versteckt. [68] Diese Information ist in Word oder Excel selbst nicht sichtbar, kann aber mit einem simplen Text-Editor, der alle Zeichen anzeigt, gelesen werden.



Mit dieser Information ist es möglich, Dokumente zu dem Rechner zurückzuverfolgen, auf dem sie geschrieben wurden, und damit oft auch zu ihrem Autor. Man kann sich leicht Szenarien ausdenken, wo dieser Mechanismus im politischen, betrieblichen oder privaten Bereich als Kontrollinstrument eingesetzt werden kann. Darüber hinaus enthalten Word-Dokumente oftmals versteckt die Geschichte ihrer Bearbeitung, was bei Verträgen oder Gutachten zu unangenehmen Konsequenzen führen kann. Interessant für die Öffentlichkeit, aber peinlich für die Schreiber erwies sich, daß in einer Machbarkeitsstudie zum Transrapid-Projekt, die man als Word-Dokument vom Server des NRW Verkehrsministerium herunterladen konnte, zu entdecken war, daß in der Endfassung einige für die Landesregierung unangenehme Punkte verändert oder weggelassen worden waren. [7]

Inzwischen sammeln und/oder transferieren immer mehr Geräte (heimlich) Daten der Nutzer. Zum Beispiel speichert der Windows Media Player 8 in einer Datei Angaben zu den DVDs, die ein Nutzer abspielt, zusammen mit einem Identifikator und übermittelt diese Daten auch an einen Microsoft-Server, wenn man nicht gerade offline ist. Bis zum Februar 2002 stand davon nichts im Privacy Statement zum Media Player, erst nachdem The Associated Press darüber berichtete, wird nunmehr erklärt, was da

[42] Für Technik-Freaks: die MAC-Adresse seiner Ethernet-Schnittstelle.

geschieht und wie man den Datentransfer unterbindet, allerdings nicht, wie man an die gespeicherten Daten rankommt oder sie wieder los wird. [74] Wie immer beteuert Microsoft, daß dies nur zum Nutzen der Nutzer geschehe und sie nicht beabsichtigten, die Daten über Nutzungsgewohnheiten zu verwerten, schließen dies aber auch nicht aus: »If users tell us that they want the ability to get recommendations, that's something we could look into on the behalf of users«.[43] [50] Die Sensibiliät von Microsofts Multimedia-Entwicklern in Fragen der Privacy wird vielleicht am besten durch folgende Äußerung kenntlich: »"If you're watching DVDs you don't want your wife to know about, you might not want to give her your password." said David Caulton, Microsoft's lead program manager for Windows Media.« [50]

Am bedenklichsten unter dem Privacy-Gesichtspunkt erscheint aber das 1999 initiierte Passport-Konzept – eines der Kernstücke der .NET-Initiative von Microsoft, das fest mit Windows XP ›verbundelt‹ ist. .NET Passport ist ein zentraler Authentifikations-Dienst, der einen »single sign-in« Mechanismus für die verschiedensten Transaktionen im Web bereitstellen soll. Bisher muß man sich bei unterschiedlichen Web-Sites, die für sichere Transaktionen die Identität des Nutzers überprüfen müssen (e-Commerce, Banken, Regierungsstellen), jeweils gesondert anmelden. Mit Passport meldet man sich nur einmal bei Microsoft an (»sign-in«), und Microsoft bestätigt dann die Identität gegenüber den mit Passport assoziierten Web-Sites. Außerdem dient Passport als ›Speicherplatz‹ für persönliche Informationen, wie Kreditkartennummer und Bankverbindungen – in sogenannten »Wallets« – und Kundendaten, die die assoziierten Websites anlegen.

Wenn man diesen Service nutzen möchte bzw. in Windows XP penetrant dazu genötigt wird, muß man eine Lizenzvereinbarung akzeptieren, deren ›Terms of Use‹ bis April 2001 vorsahen, daß man Microsoft alle Rechte an den Informationen einräumt, die man der Passport-Website übergibt bzw. übergeben muß: »by posting messages, uploading files, inputting data, submitting any feedback or suggestions, or engaging in any other form of communication with or through the Passport Web Site, you ... are granting Microsoft and its affiliated companies permission to: Use, modify, copy, distribute, transmit, publicly display, publicly perform, reproduce, publish, sublicense, create derivative works from, transfer, or sell any such communication.« [118] So grotesk es auch erscheinen mag: für alle Informationen, die man irgendwo auf der Microsoft Passport Website hinterließ, seien es Name, Adresse, Kreditkarten-Nummer, Bankverbindungen, Texte oder Kalendereinträge, für all diese Daten sollte man Microsoft unbeschränkte Nutzungsrechte gewähren. Nachdem diese Vereinbarung

[43] Die Behauptungen, daß keine »personally identifiable information« , sondern nur »machine-identifying information« übertragen würde und daß diese nicht in Verbindung mit anderen persönlichen Informationen wie Email-Adressen gebracht werden können, erscheinen zumindest dubios, entsprechen auch nicht ganz der angedeuteten Bereitschaft, dies doch »on behalf of the users« zu tun. [74] [12]

Aufsehen erregt hatte, wurde sie als dummes Versehen abgetan und die Rechteübergabe auf direkte Kommunikation mit Microsoft eingeschränkt [118], – ein für die Rechts- und Entwicklungsabteilung eines der größten Unternehmen der Welt ziemlich unverständlicher und unglaubwürdiger ›Lapsus‹.

Man kann diese ›Fehlleistung‹ aber auch mit Microsofts Wunschphantasien in Verbindung bringen: Bei einem Kreuzverhör im aktuellen Microsoft-Verfahren am 22.4.2002 kam ein vertraulicher Geschäftsplan (»MSN and Personal Services Group Business Plan«) vom Juni 2001 zur Sprache. Dort heißt es: »Passport users are the feeder pool that enables both the .NET platform and a deeper service relationship with customers.« »We will encourage Passport users to opt into our broader network services; sharing accurate demographic information with us, city, ZIP Code, age and gender so that we can create a profile for these users, allowing us to both provide a personalized experience and improve our ad targeting.« In einem »Dreams« betitelten Abschnitt findet schließlich der Vater des Gedankens beredten Ausdruck: »Create the largest and most leveragable database of profiles on the planet. A subscription relationship with every user on the Internet.« [79]

Dieser Traum wird wohl noch eine Weile Schaum bleiben, denn das Konzept ist außerhalb von Redmond bislang auf wenig Begeisterung gestoßen. [65] Das zähe Ringen um elementare Privacy-Rechte rund um Passport aber ging erstmal weiter. Im Juli 2001, also noch vor Auslieferung von Windows XP, haben dreizehn Verbraucherschutz-, Privacy-, Bürgerrechts- und Informatik-Organisationen bei der Federal Trade Commission (FTC) ein »Complaint and Request for Injunction, Request for Investigation and for Other Relief« eingereicht, in der sie »privacy implications of the Microsoft XP operating system that is to become the primary means of access for consumers in the United States to the Internet« einklagen: »As is set forth in detail below, Microsoft has engaged, and is engaging, in unfair and deceptive trade practices intended to profile, track, and monitor millions of Internet users.« [6S] Als Reaktion auf die massive Kritik von allen Seiten wurden in der Folgezeit einige der schlimmsten Auswüchse abgemildert, nach Meinung vieler Privacy-Advokaten sind die Probleme aber nicht wirklich behoben worden.[44] [5] Für die Registrierung bei .NET Passport ist minimal nur die Angabe der Email-Adresse notwendig, zusätzlich erforderliche persönliche Daten variieren je nach Dienst, den man in Anspruch nehmen will. Und während in der bemängelten Privacy Policy nur der völlig unverbindliche Satz: »All Web sites participating in the Passport program must have a posted privacy policy.« stand, wird in der (bis zum Mai 2002 aktuellen) Fassung vom 8.10.2001 von den assoziierten Anbietern ein wenig Niveau gefordert und außerdem den Nutzern gleich mehrfach

[44] Die EU-Kommission prüft zur Zeit noch, inwieweit .NET Passport gegen die EU-Datenschutzrichtlinie und europäische Datenschutzgesetze verstößt. [60]

empfohlen, deren Privacy Policies sorgfältig zu studieren: »All participating sites are required to have a posted privacy statement and to use commercially reasonable efforts to comply with industry-standard privacy guidelines and practices. ... Nevertheless, the privacy practices of .NET Passport participating sites will vary. *Therefore you should carefully review the privacy statement for each .NET Passport participating site you sign in to, in order to determine how each site or service will use the information it collects.*« [75]

Allerdings können Privacy Policies sich über Nacht ändern, natürlich auch bei Passport selbst.[45] ».NET Passport will occasionally update this Privacy Statement. ... .NET Passport encourages you to periodically review this Privacy Statement to stay informed about how we are protecting your information.[46] Your continued use of the .NET Passport Services constitutes your agreement to this Privacy Statement.« [75] Wenn man also seine Privatsphäre ernst nimmt und sich nicht automatisch mit allem einverstanden erklären will, ist man gezwungen, regelmäßig das Kleingedruckte in Privacy Policies zu überprüfen, um gegebenenfalls aus dem Dienst wieder auszusteigen, was die Bequemlichkeit des »single sign-in« Mechanismus etwas mindert.

Wie auch immer künftige Regelungen von .NET Passport aussehen mögen, und selbst wenn alle Fragen der Privacy Policy zufriedenstellend gelöst werden könnten, so bleibt das Problem der zentralen Speicherung von persönlichen Daten. Dies macht das Authentifizierungssystem zu einem ebenso reiz- wie wertvollen Angriffsziel für Cracker und Verbrecher, und es wird damit zu einer zentralen Risikoquelle. Schon im Jahre 2000 haben David Kormann und Aviel Rubin auf eine Fülle von (potentiellen) Sicherheitsschwachstellen hingewiesen [54], die Microsoft später zum Teil ausgeräumt zu haben behauptet [80]. Daß es mit der Datensicherheit in Passport aber nicht besser als bei anderen Microsoft-Produkten bestellt ist, zeigt eine Sicherheitslücke, die Marc Slemko Ende letzten Jahres aufgedeckt hat und die es ermöglichte, persönliche Daten aus den

---

[45] Es gibt genügend prominente Beispiele, daß Firmen (z.B. Amazon, Yahoo und eBay) ihren Umgang mit personenbezogenen Informationen zu Lasten der Nutzer geändert und diese teilweise eher verwirrend darüber informiert haben. Die unfeine Praxis, Privacy Policies nachträglich zu ändern, wird im Uniform Computer Information Transactions Act (UCITA; -> 9.) gesetzlich sanktioniert. Außerdem werden persönliche Kundendaten von in Konkurs geratenen Firmen – auch wenn das im Falle von Microsoft eher unwahrscheinlich ist – meist mit der Konkursmasse verkauft, worauf man als Betroffener schon gar keinen Einfluß hat. Joel Spolsky meint deshalb: »If you really trust any Internet company to protect your privacy, I've got a bridge to sell ya.« [113]

[46] Der letzte Satz ist seit Mai diesen Jahres durch den benutzerfreundlicheren Passus: »Any update to this Privacy Statement that expands the sharing or use of your personal information that you have previously provided will require .NET Passport to obtain your additional consent. For Kids Passport accounts, such additional consent will be required from the parent.« ersetzt worden. Es erscheint nicht abwegig zu vermuten, daß dies eine Reaktion auf die Untersuchung der EU-Kommission ist, weil eine einseitige Erweiterung der Verwendung von persönlichen Daten eindeutig gegen die EU-Richtlinie und Datenschutzregelungen der EU-Länder verstößt. Wie die erneute Zustimmung zu erfolgen hat, und welche Bedeutung der »continued use« jetzt hat, bleibt allerdings unklar.

Wallets zu stehlen. [111] »In a demonstration of the exploit earlier this week, Slemko sent Wired News a specially crafted but innocent-looking e-mail. Moments after the e-mail was viewed using Microsoft's Hotmail Web-based e-mail service, Slemko rattled off, over the phone, the credit card number and contact information from the user's Passport wallet.« [67] [47] Zu diesem Zeitpunkt waren nach Microsofts Angaben 200 Millionen Nutzer bei Passport registriert, und 2 Millionen hatten Wallets eingerichtet.

Eine Zentralisierung von persönlichen Daten ist aus Sicht der Nutzer in jeder Hinsicht das Dümmste, was man machen kann, – sei es wegen des Risikos eines Diebstahls und Mißbrauchs, wegen der Gefahr des Tracking und der Verwertung des ›digitalen Schattens‹, den man im Web hinterläßt, oder aus politischen Gründen im Hinblick auf Machtkonzentration und der Abhängigkeit von Monopolen. Whitfield Diffie, einer der ›Erfinder‹ der Public-Key Kryptographie, und seine Kollegin Susan Landau stellen in einem Kommentar zu »The Threat Of Microsoft's .Net« abschließend fest: »If history has shown us anything, it's that the best protection lies in decentralizing power and promoting competition. We need to take the same approach to our digital identities and make sure that who and what we are is not held captive by a single entity.« [23]

7. Wie steht Microsoft zu Open Source?[48]

Auch wenn sich Bill Gates manchmal als Pate der Open-Source-Entwicklung geriert [21], so stellt die Idee der Freien Software doch wohl das klarste Feindbild von Microsoft dar. Ende 1998 wurde Eric Raymond ein firmeninternes strategisches Memorandum zugespielt, das er kommentiert unter dem Namen »Halloween Documents« publik gemacht hat. [92] Das Papier beschäftigt sich mit Open Source Software (OSS), der von ihr ausgehenden Bedrohung der Marktführerschaft von Microsoft, insbesondere durch Linux im Server-Bereich, und möglichen Gegen-maßnahmen: »OSS poses a direct, short-term revenue and platform threat to Microsoft,

[47] Während Microsofts Adam Sohn hier »very sophisticated exploits« am Werke sah, behauptete Marc Slemko, daß er sich den Angriff in einer halben Stunde ausgedacht habe. [67]

[48] Unter Freier Software oder Open Source Software versteht man Programme, die zumeist von einem (weltweit verteilten) Kollektiv von Programmierern entwickelt werden und deren Quellcode (source code) jedermann zugänglich ist. Das wohl bekannteste Open Source Produkt ist das GNU/Linux Betriebssytem. Linux wird, wie der überwiegende Teil von Open Source Software, unter der GNU General Public Licence (GPL) vertrieben, die Richard Stallman als »Copyleft«-Vereinbarung versteht. Sie besagt, daß GPL-lizenzierte Programme im Quellcode zur freien Verfügung gestellt werden müssen, beliebig kopiert und modifiziert werden dürfen, aber jedes ›abgeleitete‹ Progamm, das GPL-Software verwendet, ebenfalls wieder unter der GPL vertrieben werden muß. Damit soll gewährleistet werden, daß kollektiv erzeugtes Wissen nicht privatisiert werden kann. Es gibt eine Fülle von anderen ›freien‹ Lizenzen, die schwächere Forderungen als die GPL stellen, um Open Source Software auch einem breiteren, proprietär engagierten Entwicklerkreis zugänglich zu machen, bis hin zur FreeBSD-Lizenz, die fast keine Auflagen für Verwendung und Weitervertrieb enthält. Eine ausgezeichnete Darstellung findet man in Volker Grassmucks Buch »Freie Software«. [44]

particularly in server space. Additionally, the intrinsic parallelism and free idea exchange in OSS has benefits that are not replicable with our current licensing model and therefore present a long term developer mindshare threat.« In der fast romantischen Darstellung des kollektiven Entwicklungsprozesses schwingt Bewunderung mit.[49] »The ability of the OSS process to collect and harness the collective IQ of thousands of individuals across the Internet is simply amazing. More importantly, OSS evangelization scales with the size of the Internet much faster than our own evangelization efforts appear to scale.« [92]

Die simple FUD-Taktik (»Fear, Uncertainty, Doubt«; -> 8.), Linux als Spielzeug von Bastlern hinzustellen, das keine Zukunft hat, erscheint dem Autor angesichts von dessen etabliertem Status nicht vielversprechend. »OSS is long-term credible ... FUD tactics can not be used to combat it.« Bessere Kampfmaßnahmen soll die Analyse liefern, unter welchen Bedingungen Open-Source Entwicklungen erfolgreich sind: »Linux can win as long as services/protocols are commodities.« Daraus ergibt sich die naheliegende Empfehlung: »De-commoditize protocols & applications. OSS projects have been able to gain a foothold in many server applications because of the wide utility of highly commoditized, simple protocols. By extending these protocols and developing new protocols, we can deny OSS projects entry into the market.« und »By folding extended functionality ... into today's commodity services, we raise the bar & change the rules of the game.« [92] Eine drastischere Selbstdarstellung von Microsofts ›embrace and extend‹-Strategie (-> 2.2) wird man schwerlich finden.

In der Folgezeit avanciert Linux zur Lieblingsbedrohung von Microsoft: »Linux is the long-term threat against our core business. Never forget that!« schreibt Brian Valentine im November 2001 in einer vertraulichen Mail an seine Verkaufsmannschaft. [45] Der Ton wird schärfer, und die Angriffe richten sich zunehmend gegen das Linux zugrunde liegende Lizensierungsmodell – die GNU General Public Licence (GPL). Es geht gegen den Geist der freien Software, nicht gegen den kollektiven IQ ihrer Vertreter, den man durchaus verwerten möchte. Bill Gates meint in einem Interview leutselig, daß freie Software eigentlich ganz nett sei, wenn nur diese Lizenz, die die arme Industrie benachteiligt, nicht wäre: »"The ecosystem where you have free software and commercial software – and customers always get to decide which they use – that's a very important and healthy ecosystem", Gates told the interviewer. But the GPL, Gates says, "breaks that cycle – that is, it makes it impossible for a commercial company to use any of that work or build on any of that work."« [96] Microsofts CEO Steve Ballmer möchte deshalb gern verhindern, daß Open Source staatlich gefördert wird und erklärt wie gewohnt nicht zimperlich: »Linux is a cancer that attaches itself in an intellectual

[49] Pikanterweise wechselte der Autor der Halloween-Dokumente, Vinod Valloppillil, später zu einer Firma, die Linux vertreibt. [90]

property sense to everything it touches. That's the way that the license works.«[50] [69] Nicht nur Krebsgeschwüre, auch freiheitliche Viren befallen die freie Markwirtschaft. Microsofts Vizepräsident Craig Mundie meinte in einem Interview: »This viral aspect of the G.P.L. poses a threat to the intellectual property of any organization making use of it« [66], und in der Lizenz einer Beta-Version des Mobile Internet Toolkit hat Microsoft die Kombination ihres Produkts mit »Potentially Viral Software« und »Publicly Available Software« verboten, worunter sie Programme verstehen, die unter einer ›offenen‹ Lizenz wie GPL, LGPL, The Artistic Licence, Mozilla Public License, Netscape Public Licence, Sun Community Source Licence oder der Sun Industry Standard License vertrieben werden. [61] [51]

Bryan Pfaffenberger erklärt die verstärkte FUD-Kampagne, die ihm »mysteriously out of proportion« erscheint, damit, daß die GPL die Firmenpolitik von Microsoft bedrohe. »I believe the GPL does pose a threat to Microsoft's business model, and that's why the free software licensing scheme is under such concerted attack. Specifically, the GPL threatens Microsoft's ability to preserve what economists and legal scholars (as well as the judge in the Microsoft antitrust case) call the "application barrier to entry"– the primary means by which Microsoft has been able to establish and preserve commanding dominance in its core markets.« [87] Dieses Geschäftsmodell besteht natürlich wesentlich darin, die Dominanz bei Betriebssytemen wie Anwendungs-Software zu erhalten und auszubauen. Dazu muß verhindert werden, daß in relevantem Maß alternative Entwicklungen und Umgebungen entstehen; »application barrier to entry« meint ja, daß Nutzer nicht auf ein anderes Betriebssystem wechseln werden, wenn ihnen dort nicht genügend viele Anwendungen zur Verfügung stehen. Wie wir gesehen haben, sind dazu ›embrace and extend‹-Strategien bestens geeignet (-> 2.2). Nun läßt aber die GPL keine proprietären Veränderungen zu. Richard Stallmann charakterisiert ihre wesentlichen Eigenschaften: »The central idea of copyleft is that we give every one permission to run the program, copy the program, modify the program, and distribute modified versions – but *not permission to add restrictions of their own*.« [115, unsere Hervorhebung] Daraus ergibt sich für den Monopolisten die unangenehme Konsequenz: »Microsoft can't play its "embrace and extend" game with GPL-licensed software because the company can't appropriate and modify the code. If Linux

[50] FUDdlerweise stellt Ballmer in diesem Interview die GPL falsch oder zumindest mißverständlich so dar, als ob eine Firma, die freien Code benutzt, alle ihre Produkte unter der GPL vertreiben müßte: »Open source is not available to commercial companies. The way the license is written, if you use any open-source software, you have to make the rest of your software open source.« [69]

[51] Bezeichnenderweise fehlt die BSD-Lizenz in der Aufzählung, da Microsoft FreeBSD-Code selbst benutzt. Nach Kritik wurde die Lizenz erstmal zurückgezogen und soll überdacht werden. Ein ähnliches Verbot findet sich in der gebührenfreien Lizenz der Dokumentation des Common Internet File System (CIFS) Protokolls, wo Entwicklungen unter sogenannten »IPR Impairing Licences« (Intellectual Property Rights) ausgeschlossen werden. [81] Es ist etwas unklar, ob damit Open-Source Projekte wie SAMBA, die eine Interoperabilität zwischen der UNIX-Welt und Microsoft-Produkten herstellen wollen, eingeschüchtert werden sollen. [18]

had been released under the BSD license, Microsoft would have probably already released a version of Linux, Linux++ or Linux# or L-Nux, with a variety of maddeningly incompatible oddities that taken together would make it even more difficult to develop applications for Linux.« [87]

8. Was bedeutet FUD?

Das Akronym FUD steht für *Fear, Uncertainty, Doubt*. »It is a marketing technique used when a competitor launches a product that is both better than yours and costs less, i.e. your product is no longer competitive. Unable to respond with hard facts, scare-mongering is used via 'gossip channels' to cast a shadow of doubt over the competitors offerings and make people think twice before using it. In general it is used by companies with a large market share, and the overall message is 'Hey, it could be risky going down that road, stick with us and you are with the crowd. Our next soon-to-be-released version will be better than that anyway'.« [51]

In den 70er Jahren war der Marktführer IBM für seine FUD-Strategien berüchtigt. Eines ihrer Opfer war Gene Amdahl, der den Ausdruck FUD geprägt hat. Amdahl war ein Ingenieur bei IBM, der sich Anfang der 70er Jahre selbständig machte und einen eigenen Prozessor ›V/6‹ konstruierte, der die IBM-Software ausführen konnte, aber erheblich schneller und billiger als vergleichbare IBM-Maschinen war. IBM kündigte daraufhin eine neue Rechnergeneration mit einem erweiterten Instruktionensatz an, der jedoch geheim gehalten wurde. Es war klar, daß Amdahls Prozessor damit nicht mehr kompatibel sein würde, und seine Aufträge gingen drastisch zurück. Die ein Jahr später herausgebrachte IBM-Maschine war zwar nach wie vor schlechter als der V/6, aber Amdahl konnte nicht Fuß fassen, und IBM baute in Folge seinen Marktanteil im Großrechnerbereich auf 97% aus. [87]

IBM übertrug die bewährten Techniken auch auf den sich ausbreitenden PC-Markt, dessen Entwicklung sie anfangs verschlafen hatten. Obwohl der IBM-PC in mancher Hinsicht schon existierenden PCs unterlegen war, konnte er sich unter den Auspizien des Giganten - »stick with us, we are big« - durchsetzen und verdrängte weitgehend den schon existierenden Markt. Microsoft lieferte nicht nur das Betriebssytem des IBM-PCs, sondern übernahm auch deren Unsitten. »Microsoft soon picked up the art of FUD from IBM, and throughout the 80's used FUD as a primary marketing tool, much as IBM had in the previous decade. They ended up outFUDding IBM themselves during the OS2 vs Win3.1 years.« [51]

In neuerer Zeit setzte Microsoft dubiose Mittel beispielsweise im Rahmen ihrer groß angelegten .NET-Initiative ein, um Anbieter und Entwickler von alternativen Ansätzen,

die auf der plattformunabhängigen Programmiersprache Java beruhen, abzuschrekken. Die elektronische Zeitschrift ZDNet UK veranstaltete Ende 2001 eine Umfrage, wer Web-Services mit welcher Technologie anzubieten gedenkt. In einem am 21. Dezember veröffentlichten Zwischenergebnis hatte eine überwältigende Mehrheit für Java-Lösungen votiert, am 5. Januar 2002 hatte sich das Verhältnis umgekehrt und dreiviertel der Einsender wollten .NET-Technologien verwenden. Es stellte sich heraus, daß die meisten der Weihnachtswähler aus dem ›microsoft.com‹-Bereich kamen, einige bis zu 228 mal zu votieren versuchten und darüber hinaus automatisierte Stimmabgaben durch Softbots eingesetzt wurden. ZDNet bemerkt dazu: »Microsoft may have shot itself in the foot this time, but future efforts may be a little more subtle.« [53]

Verbreitung von Unsicherheit wird von Microsoft ebenfalls gegen Linux, das sich vor allem im Server-Bereich zu einer ernsthaften Konkurrenz entwickelt hat, für notwendig erachtet. Auch wenn der Autor der Halloween-Dokumente (-> 7.) meinte, daß Open Source ein längerfristiges und schwer angreifbares Phänomen sei, dem man mit FUD-Taktiken (allein) nicht beikommen könne, schadet es nichts, wenn man es trotzdem versucht. Einige Zitate aus (internen) Microsoft-Dokumenten und öffentlichen Äußerungen mögen dies illustrieren.

Die Open-Source Bewegung wird als eine Vereinigung von Hobbyprogrammierern hingestellt, die keine ernsthaften Anwendungen verfolgen: »Linux often uses the catch phrase "built by users for users" but a more realistic restatement is "built by developers for developers." The Linux development community is comprised of technical hobbyists and UNIX enthusiasts whose idea of usability is a good text editor with which to modify configuration files.« [123] Oder sie mutieren von Bastlern zu wohlmeinenden Straßenräubern, die mit der großen weiten Welt nicht zurande kommen: »“Complex future projects [will] require big teams and big capital," said Ed Muth, a Microsoft group marketing manager. “These are things that Robin Hood and his merry band in Sherwood Forest aren't well attuned to do."« [49] Um die Zuverlässigkeit von Open-Source Entwicklungen in Frage zu stellen, versteigt sich das von Microsoft Deutschland verbreitete Weißpapier »Linux im Handel & Hotel- und Gaststättengewerbe. Was jeder Händler wissen sollte« gar zu der grotesken Behauptung: »”Open Source” heißt, jeder Anwender erhält eine Kopie des Quellcodes. Dabei stoßen Entwickler, die mit Linux arbeiten, häufig auf Sicherheitslücken. Auf Microsoft Windows trifft dies nicht zu.« [70] Wenn diese Behauptung einen Sinn ergeben soll, dann muß man sie wohl dahingehend interpretieren, daß bei Windows-Systemen nicht die Entwickler sondern Hacker die Sicherheitslücken bemerken.

Eine nicht zentral gesteuerte Organisation kann aus Sicht eines Monopolisten natürlich keine Vision und keine Zukunft haben: »Linux adoption and deployment is limited. No future vision with too many current choices.« [123] Das klingt etwas merkwürdig von

einer Firma, die derart viele verschiedene Versionen von Betriebssystemen und Anwendungssoftware herausgebracht hat, die vielfach nicht miteinander kompatibel sind. Vor allem aber muß die Kontinuität eines offenen, dezentralen Entwicklungsprozesses in Frage gestellt werden: »The development model is likely to fail as Linux grows into a real OS«; behaupten kann man allemal: »fragmentation - it is already happening«, und gern säht man Zweifel immer noch durch eine unschuldige Frage: »If the Linux pure plays fail, will Linux follow?« [123]

Am Gefährlichsten erscheint jedoch der Hinweis auf mögliche Konflikte des offenen Entwicklungsmodells von Open Source Software mit Urheberrechtsregelungen, weil sie eine reale Grundlage haben könnten: »Unless Linux violates IP rights, it will fail to deliver innovation over the long run.« [91] Eric Raymond bemerkt dazu: »As propaganda, it has a superficial cleverness. It plants the idea that any MIS manager so foolish as to use Linux will find his operating system yanked out from under him by a future patent lawsuit -- perhaps one initiated by (whisper it) Microsoft itself. It's a perfect FUD tactic.« [91] [52] Unsicherheit kann leicht in eine reale Bedrohung umschlagen, wenn FUD sich mit Lobby-Arbeit paart und das Zusammenspiel zwischen Großindustrie und Regierungen wie geschmiert funktioniert. Inzwischen steht in den USA ein neuer Gesetzesentwurf namens SSSCA bzw. CBDTPA zur Debatte (-> 9.), der Hersteller darauf verpflichtet, Mechanismen zum Schutz von Urheberrechten in Geräte und Software einzubauen. Wenn ein derartiges Gesetz verabschiedet wird, wird es Open-Source Entwicklungen das Leben schwer machen, unter anderem, weil man behaupten könnte, daß sich bei Source Code solche Schutzmechanismen leicht entfernen lassen. Dies wäre dann angewandte Selffulfilling Prophecy.

FUD-Taktiken sind natürlich auch im politischen Feld wirksam, und es wurde zum Beispiel versucht, den Eindruck zu erwecken, es gäbe eine Graswurzel-Initiative gegen den Microsoftprozeß. [86] Hier können auch konservative Organisationen helfend einspringen, wie die folgende Unterschriftenaktion von Richard Viguerie's ConservativeHQ.com zeigt. [97]

[52] Dies ist in den Halloween-Papers schon empfohlen worden: »The effect of patents and copyright in combatting Linux remains to be investigated.« [92]

Dieser Aufruf gegen eine »Hexenjagd« gegen Microsoft hat die interessante Eigenschaft, daß nicht klar wird, wie man *nicht* unterschreibt. Wir sind deshalb nicht sicher, ob wir das Machwerk nicht unfreiwillig unterzeichnet haben.

9. Wieso können Firmen so schlechte Software vertreiben?

Weil sie keine Produkte sondern Lizenzen verkaufen, oder wie es bei Microsoft heißt: »The Product is licensed, not sold.« [71] Beim Verkauf von materiellen Produkten gibt es in den meisten Ländern einen Verbraucherschutz, und die Hersteller haften in gewissem Umfang für durch ihre Produkte verursachte Schäden; bei Lizenzen können sich die Entwickler, teilweise in einem rechtsfreien Raum, weitgehend von Verantwortung freisprechen. Zwar gibt es immer wieder, insbesondere verstärkt in letzter Zeit, Stimmen, die auch Softwareherstellern mehr Verantwortung aufbürden wollen [4], aber faktisch geht die Gesetzgebung in die entgegengesetzte Richtung und trachtet die Interessen der großen Konzerne zu wahren und zu mehren.[53] In den USA segnet der Uniform Computer Information Transactions Act (UCITA)[54] die verbreiteten »shrink-wrap« oder »click-through« Lizenzen, die man allzuoft ungelesen akzeptiert, ausdrücklich ab und geht sogar über die bisherige Praxis hinaus.

Nach dem UCITA können Lizenzen

– jede Art von Haftung für durch Software verursachte Schäden ausschließen, gleich wie fahrlässig die Entwickler vorgegangen sind,
– Reverse Engineering[55] verbieten, auch wenn dies zur Fehlerbehebung geschieht, was nach dem Digital Millennium Copyright Act (DMCA) im Prinzip zulässig wäre,
– jede nicht explizit zugelassene Nutzung verbieten,
– das Veröffentlichen von Benchmarks[56] verbieten.

Darüber hinaus dürfen die Hersteller

---

[53] Wir beschränken uns hier auf die Entwicklung in den USA. Es ist zur Zeit schwer abzuschätzen, wie die gesetzlichen Regelungen in Deutschland und der EU endgültig aussehen werden. Frühere Erfahrungen lassen befürchten, daß Prozesse in den USA uns ebenfalls betreffen, und den technischen Inkarnationen rigider Politik ist schwer zu entgehen.

[54] UCITA ist eine Erweiterung des Uniform Commercial Code (UCC), der in etwa dem deutschen AGB-Gesetz entspricht, auf digitale Produkte. [56] Der Act ist bislang erst in zwei US-Bundesstaaten Gesetz, soll aber in weiteren übernommen werden. Zur Zeit arbeitet ein Kommitee an einigen ›entschärfenden‹ Zusätzen, es sieht aber nicht so aus, als käme dabei etwas wesentlich anderes heraus. [34]

[55] Reverse Engineering bezeichnet den Vorgang der Extraktion von Konstruktions- und Fertigungs-Know-How aus einem fertigen Produkt, also etwa die Rückübersetzung (Dekompilierung) eines ›Binaries‹ in die Programm-Instruktionen des Quellcodes.

[56] Benchmarks dienen dazu, die Performanz von Rechnern oder Programmen mit mehr oder weniger standardisierten Tests zu vergleichen.

– Vereinbarungen der Lizenz nachträglich verändern; sie müssen die Kunden nur mit einer Email benachrichtigen,
– Software (nach bestimmten Vorkehrungen) ›remote‹ über das Netz abschalten, wenn sie meinen, daß Lizenzvereinbarungen verletzt wurden, und sie haften bis auf einige Ausnahmefälle nicht für dadurch entstehende Schäden.[57]

Natürlich hat auch Microsoft solche ›Schrumpf‹-Lizenzen längst im Angebot:[58]

– Die Lizenz für Frontpage 2002 verbietet den Nutzern, mit diesem HTML-Editor Inhalte zu erstellen, die Microsoft kritisieren oder in ein schlechtes Licht stellen: »You may not use the Software in connection with any site that disparages [= verunglimpfen] Microsoft, MSN, MSNBC, Expedia, or their products or services, infringe any intellectual property or other rights of these parties, violate any state, federal or international law, or promote racism, hatred or pornography.« [15] [59] Offenbar können Lizenzen auch das verfassungsmäßig garantierte Recht der freien Rede einschränken.

– Die Lizenz für Windows XP Professional gibt Microsoft in den Product Use Rights (PUR) das Recht, Betriebssystemteile nach Belieben auf dem Rechner des Betreibers zu checken und zu ersetzen. »You acknowledge and agree that Microsoft may automatically check the version of the Product and/or its components that you are utilizing and may provide upgrades or fixes to the Product that will be automatically downloaded to your Workstation Computer.« [35] In sicherheitstechnisch sensiblen Bereichen wie Banken, Regierungsstellen oder Versicherungen werden neue Versionen und Updates erst nach monatelanger Evaluation und Prüfung installiert. Hier zu akzeptieren, daß Microsoft sich das Recht sichert, Updates ohne Wissen und Zustimmung der Betreiber in einen Rechner einzuspielen, ist vollkommen inakzeptabel. Microsoft weist zwar darauf hin, daß man den automatischen Update abstellen kann, aber es stellt sich die Frage, warum dieser Passus im PUR-Dokument (stillschweigend) hinzugefügt worden ist.

– Die ›End-User License Agreements‹ (EULA) von verschiedenen Microsoft-Produkten verbieten das ungenehm(igt)e Veröffentlichen von Benchmarks – unter anderem die EULAs von Windows 98 und .NET Framework – mit einem Passus ähnlich dem

---

[57] Die Möglichkeit einer solchen »elektronischen Selbsthilfe« erfordert natürlich, eine Hintertür zu implementieren, was allein schon ein hohes Sicherheitsrisiko darstellt, weil sie eventuell auch von Crackern benutzt werden kann. So ermöglicht der fehlerhaft programmierte Mechanismus, mit dem Microsoft die Registriernummer von Office für Mac OS X übers Netz auf Doppelverwendung überprüfen will, daß man von außen ein laufendes Word-Programm ›abschiessen‹ kann. [10]

[58] In Deutschland und anderen europäischen Ländern werden in den AGB-Gesetzen einige elementare Rechte aus der Vertragsfreiheit ausgenommen. Deshalb enthalten auch Microsoft-Lizenzen einen Vorbehalt wie »to the maximum extent permitted by applicable law« oder »local law may apply«. [71]

[59] Anscheinend sind unterschiedliche Lizenzen von Frontpage in Umlauf, die nicht alle diese Klausel enthalten. [15]

folgenden aus der Lizenz für Microsoft SQL Server Products: »You may not disclose the results of any benchmark test of either the Server Software or Client Software to any third party without Microsoft's prior written approval.« [71] Microsoft hat damit im letzten Jahr das unabhängige Competitive Systems Analysis Labor bedroht, das (trotz einer Zusammenarbeit mit Microsoft-Ingenieuren) einen für Microsoft anscheinend verheerenden Benchmark-Test mit Windows 2000 und NT durchgeführt hatte, worauf eine Veröffentlichung der Ergebnisse unterblieb. [31]

Barbara Simons, die Präsidentin des U.S. Public Policy Committee of the Association for Computing Machinery (USACM), stellt in der ACM-Stellungnahme zum UCITA fest: »We know that it is almost impossible to write bug-free software. But UCITA will remove any legal incentives to develop trustworthy software, because there need be no liability.«. [110] Und sogar viele US-bundesstaatliche Justizminister äußerten im Vorfeld des Gesetzes schwere Bedenken: »We are concerned that the policy choices embodied in these new rules seem to almost invariably favor a relatively small number of vendors to the detriment of millions of businesses and consumers who purchase computer software and subscribe to Internet services.« [58]

Die Nutzer haben schon zuvor Einschränkungen ihrer Rechte zugunsten der Profite der Konzerne durch den 1998 verabschiedeten Digital Millennium Copyright Act (DMCA) hinnehmen müssen. Der DMCA stellt Reverse Engineering und das Umgehen von Copyright-Schutzmechanismen unter Strafe: »no person shall circumvent a technological measure that effectively controls access to a work protected unter this title« [24, Sec.1201]; und er verpflichtet Provider, unzulässig bereitgestelltes urheberrechtlich geschütztes Material zu sperren oder zu entfernen, wenn sie davon Kenntnis erhalten. Zwar sind, wie auch im deutschen Urheberrecht, Ausnahmen vorgesehen: Reverse Engineering ist zulässig aus wissenschaftlichem Interesse, für Zwecke der Interoperabilität mit anderer Hard- und Software und zum Testen von Sicherheitsaspekten, aber da hierbei die Grenzen und Bedingungen zu eng und nicht recht klar sind, hat der DMCA schon mehrfach eine abschreckende Wirkung bewiesen.[60] Die Electronic Frontier Foundation (EFF) resümiert die Effekte von drei Jahren DMCA: »In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright piracy.«; der DMCA »chills free

[60] Im letzten Jahr wurde Dmitry Sklyarov, ein Angestellter einer Moskauer Software-Firma, in den USA auf Antrag von Adobe verhaftet, nachdem er auf einem Kongreß vorgetragen hatte, daß sie den recht primitiven Kopierschutz von Adobes e-Books geknackt haben. [36] In der Folge haben einige Wissenschaftler entdeckte Sicherheitslücken nicht mehr veröffentlicht, weil sie weiterhin ungefährdet in die USA reisen wollen. [27] Die Suchmaschine Google hat vor kurzem einige Webseiten eine zeitlang gesperrt, weil sie von der Scientology Sekte wegen einer Urheberrechtsverletzung gemäß DMCA dazu aufgefordert wurden. [109] Und Microsoft hat das Slashdot-Forum mit dem DMCA bedroht, weil die proprietäre Modifikation des Kerberos-Standards dort veröffentlicht wurde (-> Fußnote 15). Weitere Fälle findet man in [27].

expression and scientific research«, »jeopardizes fair use« und »impedes competition and innovation«. [27]

Drastische Einschränkungen haben die Nutzer beim statthaften ›fair use‹ hinzunehmen, der in früheren Urheberrechtsregelungen eher großzügig ausgelegt wurde, nunmehr aber weitgehend außer Kraft gesetzt werden kann, wenn Anbieter die zulässige Nutzung festlegen und technisch absichern dürfen. Der Gesetzgeber segnet hier schlicht ab, was die Techniker vormachen. Denn durch technische Schutzmaßnahmen kann man die zugelassene Art und Weise der Nutzung viel feiner regulieren und kontrollieren als durch ein Gesetz, – beispielsweise könnte man verhindern, daß Werbung auf einer DVD übersprungen werden kann.[61] Und für die Zukunft hat Microsoft ein Digital Rights Management (DRM) Betriebssystem patentiert, das auf allen Ebenen, von der Hardware bis zu Applikationen, Software und Inhalte vor unerlaubtem bzw. unerwünschtem Gebrauch schützen soll. Nachdem der Gesetzgeber mit dem DMCA das Umgehen solcher Schutzmechanismen unter Strafe stellt, soll er jetzt noch gewährleisten, daß es keine Alternativen dazu gibt. Und siehe da, in den USA liegt ein Gesetzesentwurf von Senator Hollings u.A. vor, der zuerst Security Systems Standards and Certification Act (SSSCA), inzwischen Consumer Broadband and Digital Television Promotion Act (CBDTPA) heißt, und der jeden Hersteller von Hard- und Software für »digital media devices« verpflichtet, Sicherheitstechnologie zum Schutz von urheberrechtlich geschütztem Material einzubauen. [19]

Sicherheit bedeutet nun nur noch »security for content« [107] (-> Fußnote 22), also nicht Schutz der Nutzer, sondern Schutz vor ihnen; und die gemeinsamen Anstrengungen von Konzernen und Gesetzgeber, Digital Rights Management zur Verfassung des ›Cyberspace‹ zu machen, laufen mit den Worten von Selene Makarios auf »little less than an attempt to outlaw general-purpose computers« hinaus. [43] Recht und billig sind ihnen abgedichtete Abspielgeräte für Medienkonserven, deren Vertrieb von Microsoft (und AOL) kontrolliert wird. »In the world of "convergence," where what we have seen as separate media (radio, television, movies, recorded music, books,magazines, newspapers, video games) are all "bitstreams" delivered to digital devices, the oligarchs of culture and the monopolist of software are discovering that this is the beginning of a beautiful friendship.« [83] Das phantasmagorische Netz aus DRM-Playern wird wenig mit dem guten alten Internet gemein haben. [62]

---

[61] Der Versuch, so etwas zu beseitigen, wäre nach dem DMCA strafbar, weil es sich auch dabei um ein »technological measure that effectively controls access to a work protected« handelt.

[62] Eine beeindrückende Vorschau in eine »Welt des totalen DRM« gibt Volker Grassmuck in [44a].

10. Wo soll das alles enden?

Es ist Mode geworden, das Internet mit der Metaphorik eines Ökosystems zu beschreiben und sich um dessen Gesundheit Sorge zu machen. Nachdem er die GPL als Schädling identifiziert hat, optiert Bill Gates freundlich für Artenvielfalt: »We believe there should be free software and commercial software; there should be a rich ecosystem that works around that.« [96] Und in seiner Zeugenaussage vom 22. April möchte er die Rolle eines Hegers in Anspruch nehmen: »Microsoft's Windows operating system is a key component of the PC ecosystem, and thus the health of the ecosystem depends in substantial part upon the continued health of and improvements to Windows.« [40] Doch leider gehen alle Anstrengungen von Microsoft darauf hinaus, aus dem Internet eine Monokultur zu machen. Nicht umsonst lautet ein Microsoft-Slogan: »One World, One Web, One Program«, wozu Eric Raymond gallig bemerkt: »Doesn't that sound like "Ein Volk, Ein Reich, Ein Führer" to you, too?« [94]

Nun sind homogene Populationen stärker vom Aussterben bedroht, und in Monokulturen breiten sich Schädlinge und Krankheiten schneller aus als in heterogenen Ökosystemen. Nicht wenige Autoren haben sich deshalb Gedanken über die Gefahren einer informationstechnischen Uniformität gemacht, sei es unter dem Gesichtspunkt der nationalen Sicherheit [114] oder allgemeiner im Hinblick auf die Verletzlichkeit der globalen informationstechnischen Infrastruktur: »The problem with monocultures is that they are extremely sensitive to attack. ... The relentless spread of a single platform, steadily incorporating more and more interrelated "features," marginalizes, pushes out and finally kills its ecological competition – in turn creating the very monocultures that leave the software vulnerable to subversion.« [11]

Uns erscheint ein anderer, eher ästhetischer Aspekt noch unerquicklicher: Monokulturen sind *öde*. Sollten sich die in den früheren Abschnitten skizzierten Vorstellungen von Microsoft, Regierungen und Medienkonzernen tatsächlich durchsetzen und sich .NET Services und Digital Rights Management, Instant Messaging und das Abspielen von DVDs als ›gepflegte‹ Normalität des Umgangs mit dem Computer etablieren, dann hat die Wildwest-Romantik vom virtuellen Raum der unbegrenzten Möglichkeiten, den der Barde des Internets, John Perry Barlow, besungen hat [3], endgültig ausgedient. Was von Wissenschaftlern und Computerfreaks als lizenziöse Kultur des Wissensaustauschs gedacht war, soll der Zivilisation des lizenzierten Konsums weichen. Wo wir in diesem Zivilisationsprozeß stehen, wird sich in den nächsten Jahren an einem sprachlichen Indiz beobachten lassen: Aus *Usern* werden *Consumer*. Dementsprechend wird der Computer nicht mehr als Medium gesehen werden, das die Ausdrucksmöglichkeiten seiner Nutzer unterstützt, sondern als Organ, das deren Medienverbrauch wie im Supermarkt überwacht. [43] Gleichermaßen verschiebt sich die Vorstellung vom Internet als einem zweiseitigen Kommunikationsmedium hin zu einem Zustellerdienst

von Information und Unterhaltung, was in der jüngsten Erklärung der Federal Communications Commission, »broadband Internet access services« seien als »information services« aufzufassen und damit wie Rundfunk zu (de)regulieren [29], zum Ausdruck kommt. Auch für die Medienindustrie und Politik gilt, was nach Scott Rosenbergs Einsicht Microsoft und AOL, trotz ihrer Querelen, verbindet: »*They don't like the Internet – and never have*.« [99] Wenn sie schon ihre proprietären, kontrollierbaren Netze nicht wiederhaben können, dann soll es ein Internet nach ihren Vorgaben sein. Der Filmindustrie schwebt gar dessen Redesign vor [26], und wir erinnern uns an Microsofts Traum: »Create the largest and most leveragable database of profiles on the planet. A subscription relationship with every user on the Internet.« Wenn sich das nicht verhindern läßt, kommt vielleicht die Zeit und die Not, ein neues zu gründen.

Referenzen

Wenn nicht anders angegeben, wurden alle URLs von uns im Mai 2002 überprüft.

1 Agre, P.: Red Rock Eater Digest, notes and recommendations, http://commons.somewhere.com/rre/2000/RRE.notes.and.recommenda6.html

2 Ard, S.: Microsoft, Kodak face off over Windows XP, c|net News.com, 31.7.2001, http://news.com.com/2100-1001-270911.html

3 Barlow, J.P.: A Declaration of the Independence of Cyberspace, 8.2.1996, http://www.eff.org/~barlow/Declaration-Final.html

4 BBC News Online: Software security law call,16.1.2002, http://news.bbc.co.uk/hi/english/sci/tech/newsid_1762000/1762261.stm

5 Berger, M: MIcrosoft puts more privacy in Passport, cnn.com, 14.8.2001, http://www.cnn.com/2001/TECH/internet/08/14/ms.passport.privacy.idg/

6 Berthomier, L.: Microsoft voleur de code 3D, Le Monde Informatique, 29.11.2001, http://www.weblmi.com/daily/2001/1129/condamnation.htm

7 Bleich, H.: Transrapid-Gutachten manipuliert? Word-Änderungshistorie zeigt gelöschte Passagen in politisch brisanter Studie, c't 2002, Heft 5, S. 41

8 Bridis, T.: XP vulnerable to hackers, CNEWSTechNews, 20.12.2001, http://www.canoe.ca/CNEWSTechNews0112/20_windows-ap.html

9 Byron Acohido, B.: Companies cringe at Microsoft licensing, USA Today, http://www.usatoday.com/usatonline/20020513/4105463s.htm

10 c't: Patch für Office v. X beseitigt Abschussgefahr, c't 2002, Heft 5, S. 39

11 Cascio, J.: The ecology of viruses, salon.com, 7.4.1999, http://www.salon.com/tech/feature/1999/04/07/melissa/

12 Caulton, D.: Microsoft response to the Windows Media Player 8 Privacy Advistory, http://www.computerbytesman.com/privacy/wmp8response.htm

13 CEI Computer Economics, www.computereconomics.com

14 CERT® Incident Note IN-2000-07: Exploitation of Hidden File Extensions, updated 27.7.2000, http://www.cert.org/incident_notes/IN-2000-07.html

15 CmdrTaco: MS FrontPage Restricts Free Speech II, 21.9.2001, http://slashdot.org/articles/01/09/21/1438251.shtml

16 CNET News.com: The Gatekeeper, 17. - 25.10.2001, http://news.com.com/2009-1001-274475.html *als pdf-Datei*: http://news.cnet.com/i/ne/en/2001/10/xp/xp.pdf

17 Complaint and Request for Injunction, Request For Investigation and for Other Relief, 26.7. 2001, http://www.epic.org/privacy/consumer/MS_complaint.pdf

18 ComputerWire: Microsoft anti-GPL fine print threatens competition, The Register, 17.4.2002, http://www.theregister.co.uk/content/59/24885.html

19 Consumer Broadband and Digital Television Promotion Act, 21.3.2002, http://cryptome.org/broadbandits.htm

20 Cooper, C.: Q & A: Steve Ballmer – trust Microsoft, ZDNet UK Tech Update, 6.2.2002, http://news.zdnet.co.uk/story/0,,t274-s2103875,00.html

21 Cringely, R.X.: Bill to Linus: You Owe ME. Did Bill Gates Invent Open Source Software? No, But He'll Take Credit For It, Anyway, The Pulpit, 22.11.2001, http://www.pbs.org/cringely/pulpit/pulpit20011122.html

22 Department of Justice: JUSTICE DEPARTMENT CHARGES MICROSOFT WITH VIOLATING 1995 COURT ORDER, 20.10.1997, http://www.usdoj.gov/atr/public/press_releases/1997/1235.htm

23 Diffie, W., Landau, S.: The Threat Of Microsoft's .NET, On#Sun.com Magazine, Dezember 2001/Januar 2002, http://www.sun.com.au/news/onsun/2001-12/microsoft_threat.html

24 Digital Millennium Copyright Act (DMCA), Final joint version of H.R. 2281, 28.10.1998, http://www.the-eggman.com/writings/dmca.html

25 Don Davidson Computer: Common Destructive Viruses in Circulation
http://home.earthlink.net/~doniteli/index15.htm

26 EFF: Consensus at Lawerpoint?: Hollywood wants to plug the “analog hole”, 23.5.2002,
http://bpdg.blogs.eff.org/archives/000113.html

27 EFF: Unintended Consequences: Three Years under the DMCA, 3.5.2002,
http://www.eff.org/IP/DMCA/20020503_dmca_consequences.pdf

28 eWeek: Microsoft: XP 'Dramatically More Secure', 22.10.2001,
http://www.eweek.com/print_article/0,3668,a=16895,00.asp

29 Federal Communications Commission: Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 15.2.2002,
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-42A1.doc

30 Festa, P., Wilcox, J.: Microsoft criticized for lack of software security, c|net News.com, 5.5.2000,
http://news.cnet.com/news/0-1003-200-1823167.html

31 Fontana, J.: Microsoft gets tough with independent testers, itworld.com,
http://www.itworld.com/AppDev/136/NWW010312118166/pfindex.html

32 Forno, R.: MS 'Security Framework' is another .NET vulnerability, The Register, 14.11.2001,
http://www.theregister.co.uk/content/55/22816.html

33 Forno, R.: MS security memo a mere gesture, The Register, 17.1.2001,
http://www.theregister.co.uk/content/4/23727.html

34 Foster, E.: Bride of UCITAstein, InfoWorld, 11.1.2002,
http://www.infoworld.com/articles/op/xml/02/01/14/020114opfoster.xml

35 Foster, E.: Check the fine print, InfoWorld, 8.2.2002,
http://staging.infoworld.com/articles/op/xml/02/02/11/020211opfoster.xml

36 Free(d) Dmitry Sklyarov!, http://www.freesklyarov.org/

37 futurezone orf.at: Microsoft drängt Kunden in Abo-Verträge, 3.6.2002,
http://futurezone.orf.at/futurezone.orf?read=detail&id=121704

38 Galli, P.: Automatic Updates Give XP Users New Headaches, eWeek,14.1.2002,
http://www.eweek.com/article/0,3658,s%253D701%2526a%253D21023,00.asp

39 Gannis, M.:The Worm Returns: CAIDA Researchers Track New Infestations of "Code Red", 8.8.2001
http://www.npaci.edu/online/v5.16/wormreturns.html

40 Gates, B.: Direct Testimony of Bill Gates, April 2002,
http://www.microsoft.com/presspass/trial/mswitness/2002/billgates/billgates.asp
als pdf-Datei: http://seattletimes.nwsource.com/art/microsoft/pdf/Gates_direct.pdf

41 Gates, B.: Trustworthy computing, 15.1.2002, email to “Microsoft and Subsidiaries: All FTE”, wiedergegeben in [46]

42 Gibson, S.: Why Windows XP will be the Denial of Service Exploitation Tool of Choice for Internet Hackers Everywhere, 21.3.2002, http://grc.com/dos/winxp.htm

43 Godwin, M.: Hollywood vs. the Internet. Why entertainment companies want to hack your computer, reasononline, Mai 2002, http://www.reason.com/0205/fe.mg.hollywood.shtml

44 Grassmuck, V.: Freie Software.Zwischen Privat- und Gemeineigentum, Bonn 2002

44a Grassmuck, V.: Mit ein bißchen Zuckerbrot und viel Peitsche in eine Welt des totalen DRM, erscheint 2002 in Telepolis

45 Greene, T.C.: MS promotes Linux from threat to ‘the’ threat - Memo, The Register, 12.11.2001,
http://www.theregister.co.uk/content/4/22770.html

46 Greene, T.C.: MS’ highes priority must be security - Billg, The Register, 17.1.2002,
http://www.theregister.co.uk/content/4/23715.html

47 Guninski G.: IE GetObject() problems, security advisory # 52, 1.1.2001,
http://www.guninski.com/getob3.html

48 heise online: Sicherheitslücke bei digitalen Visitenkarten in Outlook, 23.2.2001,
http://www.heise.de/newsticker/data/pab-23.02.01-000/

48a heise online: Bill Gates hält modulares Windows grundsätzlich für machbar, 25.4.2002,
http://www.heise.de/newsticker/data/wst-25.04.02-002/

49 Helm, L.: The 'No Secrets' Software Strategy, latimes.com, 28.12.1998, http://www.pactechcom.com/clips/ no_secrets_software_strategy.pdf

50 Hopper, D.I.: Microsoft Media Player Logs Choices, washingtonpost.com, 20.2.2002, http://www.it-c.dk/~ninarose/digitalfreedom/Microsoft%20Media%20Player%20Logs%20Choices%20(washingtonpost_com).htm

51 Irwin, R.: What is FUD?, 1998, http://www.cavcomp.demon.co.uk/halloween/fuddef.html

52 Jackson, T. P.: Findings of Fact, 5.11.1999, http://usvms.gpo.gov/ms-findings2.html

53 Judge, P.: .NET vote rigging illustrates importance of Web services, 9.1.2002, http://news.zdnet.co.uk/story/0,,t269-s2102244,00.html

54 Kormann, D.P., Rubin, A.D.: Risks of the Passport Single Signon Protocol, http://avirubin.com/passport.html

55 Krim, J.: Palm Official Says Microsoft Hinders Access, washingtonpost.com, 29.3.2002, http://www.washingtonpost.com/ac2/wp-dyn/A33532-2002Mar28?language=printer

56 Kunze, C.A.: UCITA Online, 2000, http://www.ucitaonline.com/ -> Uniform Computer Information Transactions Act, (Amended 2001) 23.8.2001, http://www.law.upenn.edu/bll/ulc/ucita/ucita01.htm

57 Lemos, R.: Wanted: Evidence of MS security push, ZDNet UK News, 4.3.2002, http://news.zdnet.co.uk/story/0,,t269-s2105503,00.html

58 Letter to NCCUSLfrom Attorneys General Opposing UCITA, 23.7.1999, http://www.arl.org/info/frn/copy/agoppltr.html

59 Lettice, J.: Compulsory Windows: for Macs, and people without PCs?, The Register, 7.5.2002, http://www.theregister.co.uk/content/4/25179.html

60 Lettice, J.: EU looks at MS Passport for privacy infringement, The Register, 24.5.2002, http://www.theregister.co.uk/content/4/25433.html

61 Lettice, J.: Open source terror stalks Microsoft's lawyers, The Register, 25.6.2001, http://www.theregister.co.uk/content/archive/19953.html

62 Lettice, J.: US DoJ rep moves to blunt Europe's action on MS, The Register, 20.5.2002, http://www.theregister.co.uk/content/4/25348.html

63 Leyden, J.: Virus writers are industrial terrorists - MS, The Register, 23.10.2001, http://www.theregister.co.uk/content/56/22423.html

64 Mackie, A., Roculan, J., Russell, R., Van Velzen, M.: Nimda Worm Analysis, Incident Analysis Report Version 2, 21.9.2001, SecurityFocus, http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf

65 Markoff, J.: Microsoft Has Shelved Its Internet 'Persona' Service, nytimes.com, 11.4.2002, http://www.nytimes.com/2002/04/11/technology/11NET.html?pagewanted=print; *erfordert eine Anmeldung*

66 Markoff, J: Microsoft is Set to Be Top Foe of Free Code, The New York Times, 3.5.2001, http://www.nytimes.com/2001/05/03/technology/03SOFT.html?pagewanted=print; *erfordert eine Anmeldung*

67 McWilliams, B.: Stealing MS Passport's Wallet, WiredNews, 2.11.2001, http://www.wired.com/news/print/0,1294,48105,00.html

68 Methvin, D.: Windows 98 knows who you are, BYTE.com, 6.9.1999, http://www.byte.com/documents/s=146/byt19990906s0012/

69 Microsoft CEO takes launch break with the Sun-Times, Chicago Sun-Times, 1.6.2001, http://www.suntimes.com/output/tech/cst-fin-micro01.html

70 Microsoft Deutschland: Linux im Handel & Hotel- und Gaststättengewerbe. Was jeder Händler wissen sollte, Weißpapier, Februar 2001 http://www.microsoft.com/germany/partner/produkte/server/windows2000server/files/Linux_Retail_WhitePaper_Deutsch.doc

71 Microsoft: End User License Agreement - Server License for Microsoft SQL Server 2000 Products, 4.2.2002, http://www.microsoft.com/sql/howtobuy/servlicense.asp

72 Microsoft: HotFix & Security Bulletin Service, http://www.microsoft.com/technet/security/current.asp

73 Microsoft: Living Our Values, 22.9.1999, http://www.microsoft.com/mscorp/values.htm

74 Microsoft: Media Player for Windows XP Privacy Statement, http://www.microsoft.com/windows/windowsmedia/software/v8/privacy.asp

75 Microsoft: Microsoft .NET Passport Privacy Statement, http://www.passport.com/Consumer/PrivacyPolicy.asp?PPlcid=1033

76 Microsoft: Microsoft Inductive User Interface Guidelines, 9.2.2001, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwindev/html/iuiguidelines.asp

77 Microsoft: OL2000: Information About the Outlook E-mail Security Update (Q262631), http://support.microsoft.com/default.aspx?scid=kb;EN-US;q262631

78 Microsoft: OL97: General Information About Using VBScript with Outlook (Q167138), http://support.microsoft.com/support/kb/articles/Q167/1/38.ASP

79 Microsoft: PressPass: UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA, 22.4.2002, http://www.microsoft.com/presspass/legal/apr02/04-22ntranscriptam.asp

80 Microsoft: Response to Kormann & Rubin Document, http://www.passport.com/Press/RubinKormann.asp?lc=1033

81 Microsoft: Royalty-Free CIFS Technical Reference License Agreement, http://msdn.microsoft.com/library/en-us/dnkerb/html/Finalcifs_LicenseAgrmnt_032802.asp

82 Microsoft: Special Edition-Office News Service-Virus Alert, 8.5.2000, http://archives.neohapsis.com/archives/microsoft/technet/2000-05/0002.html

83 Moglen E.: Gates at Appomattox: Why the US Surrendered, 9.9.2001, http://emoglen.law.columbia.edu/my_pubs/microsoft-surrender.html

84 Mugan, C.; Microsoft removes Java from latest version of Windows XP; ComputerWeekly, 19.7.2001, http://www.cw360.com/bin/bladerunner?REQUNIQ=1006280624&REQSESS=cJ95Q321& *erfordert ein Paßwort*

85 Mullen, T.: Charney an Ominous Microsoft Pick, BusinessWeek online, 14.2.2002, http://www.businessweek.com/technology/content/feb2002/tc20020213_8924.htm

86 Newsbytes: Dead People, Fake Letters, Support Microsoft - Report, infowar.com, 23.8.2001, http://www.infowar.com/law/01/law_082301c_j.shtml

87 Pfaffenberger, B.: Why is Microsoft Attacking the GPL?, LINUX JOURNAL, 27.6.2001, http://www.linuxjournal.com/article.php?sid=5058

88 Raymond, E. (Ed): Jargon File, http://www.cnam.fr/Jargon/jargon.html?602

90 Raymond, E.: Halloween Document IV: When Software Things Were Rotten, http://www.opensource.org/halloween/halloween4.html

91 Raymond, E.: Halloween Document III. Microsoft's Reaction to the Halloween Document, 1.10.1999, http://www.opensource.org/halloween/halloween3.html

92 Raymond, E.: The Halloween Document I und II, 30.10./1.11.1998, http://opensource.org/halloween/halloween1.html und .../halloween2.html

93 Raymond, E.: The Halloween Documents: An Appreciation, 20.12.1998, http://www.tuxedo.org/~esr/not-the-osi/halloween-rant.html

94 Raymond, E.: The Halloween Nightmare, 28.11.1998, http://www.tuxedo.org/~esr/not-the-osi/halloween-nightmare.html

95 Regan, T.: Microsoft on a mission, 25.10.2001, http://www.csmonitor.com/2001/1025/p11s1-stct.html

96 Ricciuti, M.: Gates wades into open-source dabate, c|net News.com, 19.6.2001, http://news.com.com/2100-1001-268667.html?legacy=cnet&tag=tp_pr

97 Richard Viguerie's Conservative HQ.com, http://www.conservativehq.com/012402.htm

98 Richter, T.: Du sollst keine anderen Player haben neben meinem, Telepolis, 18.3.2002, http://www.telepolis.de/deutsch/inhalt/co/12054/1.html

99 Rosenberg, S.: Assimilating the Web, salon.com, 26.6.2001, http://www.salon.com/tech/feature/2001/06/26/locking_up_the_web/print.html

100 Rosenberg, S.: The devil is in Windows' details, salon.com, 8.10.2001, http://www.salon.com/tech/col/rose/2001/10/08/file_monopoly/print.html

101 Rosencrance, L.: Bug-reporting standards proposed to IETF, Computerworld, 22.2.2002, http://www.computerworld.com/securitytopics/security/story/0,10801,68558,00.html

102 Ruffin, O.: Microsoft, terrorism, and computer security, The Register, 14.12.2001, http://www.theregister.co.uk/content/4/23418.html

103 SANS Institute: The Twenty Most Critical Internet Security Vulnerabilities, 1.10.2001, http://www.sans.org/top20.htm

104 Schneier, B., Shostack, A.: Results, Not Resolutions. A guide to judging Microsoft's security progress, SecurityFocus, 24.1.2002, http://online.securityfocus.com/news/315

105 Schneier, B.: Con: Trust, but verify, Microsoft's pledge, c|net News.com, 18.1.2002, http://news.com.com/2010-1078-818611.html

106 Schneier, B.: The Process of Security, Information Security, April 2000, fhttp://www.infosecuritymag.com/articles/april00/columns_cryptorhythms.shtml

107 Security Systems Standards and Certification Act, Staff Working Draft, 6.8.2001, http://cryptome.org/sssca.htm

108 Seiter, Ch.: New approach to spreadsheets uses graphical programming style, September 1996, http://www.macworld.com/1996/09/reviews/2613.html

109 Sherman, C.; Google Makes Scientology Infringement Demand Public, Search Engine Watch, 15.4.2002, http://searchenginewatch.com/searchday/02/sd0415-google-dmca.html

110 Simons, B.: Shrink-Wrapping Our Rights, August 2000, http://www.acm.org/usacm/copyright/ucita.cacm.htm

111 Slemko, M.: Microsoft Passport to Trouble, 5.11.2001, http://alive.znep.com/~marcs/passport/

112 Smith, R.M.: Security Memo to Bill Gates, 17.1.2002, http://www.computerbytesman.com/security/bill1.htm

113 Spolsky, J.: Does Issuing Passports Make Microsoft a Country?, 26.7.2000, http://www.joelonsoftware.com/articles/fog0000000047.html

114 Strassmann, P.A.: Microsoft: A U.S. Security Threat, Computerworld, 30.11.1998, http://www.strassmann.com/pubs/cw/ms-security.shtml

115 Suarez-Potts, L.: Interview with Richard Stallman, 2001, http://www.gnu.org/philosophy/luispo-rms-interview.html

116 Sutherland, E.: Intel, MS See Soft Wi-Fi Future, 1.5.2002, http://www.80211-planet.com/columns/article/0,4000,1781_1026261,00.html

117 Thurrott, P.: Windows XP Tips ‘n’ Tricks, http://www.winsupersite.com/showcase/windowsxp_tips.asp

118 Trott, B.: Microsoft alters Passport terms of use, InfoWorld, 5.4.2001, http://www.infoworld.com/articles/hn/xml/01/04/05/010405hnpassport.xml?p=br&s=1

119 Vahldiek, A.: Selbstbeschränkung. Windows XP sicher nutzen, c’t 2002 Heft 11, S. 138-143

120 Vaughan-Nichols, S.: Ban Outlook – now, 25.7.2001, http://www.zdnet.com/filters/printerfriendly/0,6061,2814683-92,00.html

121 Wilcox, J.: Microsoft reveals antitrust testimony, ZDNet News, 4.3.2002, http://zdnet.com.com/2100-1104-850976.html

122 Winer, D.: More Smart Tags, 8.6.2001, http://scriptingnews.userland.com/backIssues/2001/06/08

123 Zymaris, C.: Analysis of Microsoft's 'Competing with Linux' Document, 20.12.2001, http://www.cyber.com.au/users/conz/on_competing_with_linux_analysis.html