In diesem Kapitel:

- Caching und History
- Firefox
- Internet Explorer
- Opera
- Browserkonfiguration prüfen

KAPITEL 5

Browser – einer für alles

Eigentlich handelt es sich bei Browsern um Programme, mit denen man Webseiten betrachten kann. Technisch gesehen sind sie also Software-Clients, die den WWW-Dienst auf Webservern im Internet oder in lokalen Netzen abfragen. Die Browser der heutigen Generation sind jedoch wahre Alleskönner: Sie können mit ihrer Hilfe Programme per FTP herunterladen, E-Mails lesen und schreiben, News per RSS abonnieren, Videos ansehen, Spiele spielen, Ihr Betriebsystem auf den neuesten Stand bringen, XML Dokumente öffnen, 3-D-Animationen betrachten und vieles mehr.

Auf den ersten Blick sieht dies nach einer positiven Entwicklung aus, da man mit einer vertrauten Oberfläche die wichtigsten Internetangebote ansprechen kann. Die Verbindung dieser eigentlich voneinander völlig unabhängigen Komponenten bringt aber mehr Nachteile als Vorteile mit sich. Ist beispielsweise die Implementierung eines HTML-Befehls im eigentlichen Browserteil fehlerhaft, wirkt sich dies auch auf das integrierte E-Mail-Programm aus, denn der Hersteller benutzt die gleiche HTML-Implementierung in beiden Komponenten. Im günstigsten Fall bewirkt dies unschöne Darstellungsfehler, häufig kommt es aber zu Abstürzen und immer öfter sogar zu massiven Sicherheitslöchern, durch die ein Angreifer das ganze System unter seine Kontrolle bringen kann.

Das wohl berühmteste Beispiel für die negativen Folgen einer solchen omnipotenten Software ist sicherlich der Internet Explorer. Microsoft implementierte in diesem Produkt nicht nur Browser, FTP-, News- und Mailtools, sondern auch die hauseigene Programmiersprache Visual Basic. Mit ihr kann man Webseiten dynamisch gestalten, ihnen spürbar mehr Zugriff auf das System geben oder Funktionen in Windows automatisieren. An dieser Stelle wird auch das volle Ausmaß dieses Problems deutlich: Dieselbe Programmiersprache und dieselben Schnittstellen dienen also zugleich der Webprogrammierung sowie der Steuerung des Betriebssystems und des Office-Pakets. Grundsätzlich ist es etwas Positives, die gleiche Programmiersprache für alle Komponenten benutzen zu können, das Problem liegt aber

darin, dass Code, dem es gelingt, die Restriktionen des Browsers zu umgehen, vollen Zugriff auf Systemfunktionen erhält. Das bedeutet, dass beispielsweise ein Internet-Wurm über Ihren Browser Zugriff auf zentrale Komponenten des Betriebssystems bekommen könnte, während Sie eine infizierte Webseite anschauen. Der berühmte *I LOVE YOU*-Virus nutzte genau diese Verquickung aus, um seine Wirkung zu entfalten. Der eigentliche Virus war als Attachment an eine Mail angefügt. Dabei handelte es sich um eine *.vbs*-Datei (*Visual Basic Script*, einer mit Visual Basic verwandten Scriptsprache), in der sich der Quell-Code des Virus befand. Öffnete ein Benutzer die Datei per Doppelklick, wurde der darin enthaltene Code ausgeführt, der mit einigen Visual Basic-Befehlen das E-Mail-Programm anwies, allen Personen im Adressbuch den Virus per E-Mail zu schicken. Wäre aus dem Dateinamen des Attachments ersichtlich, dass es sich um eine *.vbs*-Datei handelt, würde wohl kaum jemand diesen Anhang öffnen. Leider ist das Windows-Betriebssystem jedoch standardmäßig so eingestellt, dass es »bekannte Dateiendungen« unterdrückt (siehe dazu auch Kapitel 3, *Sicherheitsbewusstsein*). Die verräterische Endung *.vbs* wird deshalb für den Benutzer gar nicht sichtbar und glaubt darum z.B. ein Bild oder Ähnliches vor sich zu haben.

Wie eingangs erwähnt, können sich moderne Würmer inzwischen teilweise schon beim bloßen Besuch einer Internetseite in einem Rechner einnisten und daher deutlich schneller deutlich mehr Schaden anrichten. Bedenkt man nun, dass man moderne Browser eben nicht nur zum Surfen, sondern für die meisten Online-Aktivitäten nutzt, zeigt sich schnell, wie kritisch eine Sicherheitslücke in einer so mächtigen Komponente ist. Um einer gerichtlich angedrohten Entkoppelung von Windows und Internet Explorer zu entgehen, hat Microsoft den Browser so tief in das Betriebsystem integriert, dass sich der oben beschriebene Effekt nochmals verstärkt. Wenn Sie sich ein Bild davon machen möchten, an welchen unerwarteten Stellen sich der Internet Explorer verbirgt, können Sie, wie in Abbildung 5-1 gezeigt, als kleines Experiment den Arbeitsplatz oder Windows Explorer öffnen und dort in die Adressleiste statt des Pfads zu einem Ordner eine Internetadresse eintippen. Sie werden feststellen, dass sich die angegebene Website in Ihrem Dateimanager öffnet. Das Gleiche funktioniert übrigens auch andersherum: Wenn Sie den Internet Explorer starten und in die Adressleiste einfach `C:`eingeben, öffnet sich Ihr Windows Explorer und zeigt Ihnen die Dateien auf Ihrer Festplatte an.

Verallgemeinernd kann man sagen, dass im Bereich Software – wie auch im wirklichen Leben – Monokulturen sehr anfällig für Schädlinge sind. Wenn Sie für verschiedene, eigentlich völlig unabhängige Funktionen ein einziges Programm verwenden, vererben sich die Fehler der einzelnen Komponenten weiter und gefährden im Ernstfall auch gleich das ganze System. Es sollte also in Ihrem Interesse sein, Browser, E-Mail-Programm und FTP-Client voneinander getrennt zu halten. Als gutes und nebenbei kostenloses Team hat sich beispielsweise die Kombination aus Opera (*http://www.opera.com*) oder Firefox (*http://www.mozilla.org*) als Browser, Thunderbird (*http://www.mozilla.org*) als E-Mail-Tool und Filezilla (*http://filezilla.*

Abbildung 5-1: Hinter dem Arbeitsplatz verbirgt sich in Wahrheit der Internet Explorer.

sourceforge.net) als FTP-Client erwiesen. Der Fairness halber sei hier jedoch ausdrücklich darauf hingewiesen, dass Open Source-Lösungen wie der Firefox-Browser keineswegs per definitionem sicherer sind als kommerzielle Produkte. Auch wäre es falsch, jede Software, die das Emblem von Microsoft trägt, zu verteufeln. Tatsache ist jedoch, dass verwunderlicherweise die kleinen und im Vergleich zu Micosoft personaltechnisch völlig unterbesetzten Projekte wesentlich schneller mit entsprechenden Updates auf Sicherheitslücken reagieren und den Riesen aus Redmond technologisch um Jahre abgehängt haben.[1] Letzteres gilt vor allem für Opera, jedoch ist selbst der sehr junge Browser Firefox dem in die Jahre gekommenen Internet Explorer deutlich überlegen.

Da Sie als Endbenutzer leider nur sehr wenig gegen gefährliche Sicherheitslücken unternehmen können, sollten Sie stets bemüht sein, die allerneueste Version Ihres Stammbrowsers zu benutzen. Das hat zwei Vorteile: Erstens hat der Hersteller bekannte Sicherheitslücken gestopft, zweitens sind die in der neuen Version hinzugekommenen Fehler in der Crackerszene noch nicht so bekannt.[2]

1 Aus diesem Grund wird Microsoft 2006, entgegen der ursprünglichen Planung, Version 7 des Internet Explorers als Stand-alone-Variante auf den Markt bringen. Dieser soll dann auch *tabbed browsing* unterstützen, eine Technologie, die es erlaubt, mehrere Webseiten in Unterfenstern des Bowsers zu öffnen. Opera und Firefox können dies schon seit langem. Ebenso soll das Sicherheitskonzept grundlegend erneuert werden.

2 Die Verwendung der neuesten Version einer Software hat allerdings nicht nur Vorteile: Zum einen enthalten neue Versionen in manchen Fällen durchaus dieselben Lücken wie die alten (und unter Umständen noch eine ganze Menge mehr). Zum anderen kommen mit einer neuen Version häufig Unmengen neuer Funktionen hinzu, die zwar von zweifelhaftem Gebrauchswert sind, dafür aber umso bessere Einfallstore für Angriffe darstellen. Einzige Lösung für dieses Dilemma ist es, sich gut darüber zu informieren, welche Lücken die jeweils neue Version schließt und welche neuen Gefahren bekannt sind.

Eine weitere gefährliche Eigenschaft moderner Browser ist der permanente Versuch, dem Benutzer so viel Arbeit wie möglich abzunehmen. Wir haben dieses Problem bereits in Kapitel 3, *Sicherheitsbewusstsein*, angesprochen. Tappen Sie nicht in dieses Sicherheitsloch hinein und erlauben Sie dem Browser auf keinen Fall, Ihre Kennwörter oder Formulardaten zu speichern. Wenn Sie an einem Mehrbenutzerarbeitsplatz sitzen oder sich womöglich einen gemeinsamen Account mit anderen Benutzern teilen, ist dies umso wichtiger.

Im Folgenden wollen wir uns zunächst das Caching und die History-Funktion von Browsern anschauen, da diese für Ihre Privatsphäre von entscheidender Bedeutung sein können, und anschließend einen detaillierteren Blick auf die einzelnen Browser werfen. Dabei werden wir bei jedem Produkt eine kurze Übersicht wichtiger Einstellungen geben und Empfehlungen zum Umgang damit aussprechen.

Caching und History

Nahezu alle Browser sammeln Informationen über Ihr Surfverhalten. Dabei werden neben den Cookies, die Sie zugelassen haben, auch Informationen gesammelt, von denen Sie nichts wissen. Mittels der so genannten *History-Funktion* speichert der Browser die von Ihnen besuchten Webseiten als kurze Vermerke ab. So können Sie beispielsweise nachschauen, wo Sie vor einer Woche gesurft haben. Wenn nicht ausgeschlossen werden kann, dass auch andere den Computer benutzen, sollten Sie diese Informationen regelmäßig löschen. Andererseits hat die Verlaufs- bzw. History-Funktion auch ihre Vorteile, da sie beispielsweise versucht, einmal eingegebene Adressen zu erraten, und so Tipparbeit spart.

Ähnlich verhält es sich mit dem *Cache*. Die Aufgabe des Cache besteht darin, einmal heruntergeladene Internetseiten und Bilder auf der Festplatte zu speichern und so den wiederholten Zugriff auf diese Daten erheblich zu beschleunigen. Dieser Ansatz stammt aus einer Zeit, in der das Herunterladen von Bildern eine sehr zeitintensive Aufgabe war. In den Zeiten von DSL hat der Cache zwar an Bedeutung verloren, bleibt jedoch wichtig, um die Auslastung des Internets möglichst gering zu halten und nicht jedes Mal mit den gleichen Daten die Leitungen zu verstopfen. Aus Sicherheitssicht hat der Cache den Nachteil, dass andere Benutzer des gleichen Computers nachvollziehen können, welche Internetseiten Sie besucht haben. Wenn Sie das verhindern möchten, sollten Sie den Cache regelmäßig löschen.

Um sich einen Überblick zu verschaffen, welche Daten Sie auch nach dem Surfen auf Ihrer Festplatte hinterlassen, können Sie sich nach dem Besuch einiger Webseiten mit dem Internet Explorer das Verzeichnis *C:\Dokumente und Einstellungen\Ihr-Profil\Lokale Einstellungen\Temporary Internet Files* anschauen.

Firefox

Firefox gehört zusammen mit Mozilla und dem Netscape Navigator zur Mozilla-Browserfamilie. Alle drei Browser haben weitestgehend denselben technologischen Kern, werden jedoch von verschiedenen Firmen weiterentwickelt. Die Firma Netscape wurde 1998 vom heute weltgrößten Internetprovider AOL übernommen. Der Netscape-Browser galt lange Zeit als das beste Produkt am Browsermarkt und hatte dementsprechend die weiteste Verbreitung. Das Web verdankt Netscape viele Fortschritte im Bereich der Skriptsprachen (JavaScript) und neuer, innovativer HTML-Tags. Seitdem die Browser aber kostenlos geworden sind und Microsoft seinen Internet Explorer zu einem untrennbaren Bestandteil seines Betriebssystems gemacht hat, hat der Navigator an Bedeutung verloren. AOL gab den Code daraufhin frei und die Mozilla-Community begann mit einer Komplettüberarbeitung des Quell-Codes. Das Ergebnis war die Mozilla-Suite mitsamt integrierten Mail- und Chatfunktionen. AOL entwickelte auf der Basis der Mozilla-Veröffentlichungen in unregelmäßigen Abständen neue Netscape-Versionen. Derzeit aktuell ist Version 8, die jedoch nur noch rund 1% Marktanteil hat. Die Mozilla-Community begriff jedoch frühzeitig, dass der über Jahre gewachsene Quell-Code kaum noch zu warten war und die Verquickung vieler Komponenten zu mehr Problemen als Vorteilen führte. Man entschloss sich daher, einfache, aber effektive Einzellösungen zu entwickeln, die nur noch das tun sollten, wofür sie da waren. So entand Firefox als Browser und Thunderbird als entsprechender Mail-Client. Die Mozilla-Suite wird unter dem Projektnamen SeaMonkey weiterentwickelt.

Trotz dieser Umstellungen liegt allen drei Produkten der gleiche Kern zugrunde und sie unterscheiden sich auch im Funktionsumfang sowie der Bedienung weniger voneinander, als man vielleicht erwarten könnte. Der Marktanteil von Firefox liegt weltweit etwa bei 10-12%. In Europa ist er jedoch deutlich höher und erreicht in einigen Ländern sogar Werte von über 20% (wie beispielsweise in Deutschland und Polen) oder gar 30% (in Finnland).[3]

Wir wollen uns stellvertretend für die Mozilla-Familie Firefox in der Version 1.0.7 anschauen.[4] Firefox hat einen waren Hype im Internet ausgelöst, der sehr deutlich zeigte, wie frustriert und verärgert die Internet Explorer-Benutzer waren. Anders ist nicht zu erklären, dass Firefox Microsoft innerhalb kürzester Zeit große Marktanteile abnehmen konnte. Bedenken Sie, dass 10-12% Marktanteil im Internet gleichbedeutend mit vielen Millionen Nutzern sind. In jüngster Zeit hat Firefox jedoch auch viele negative Schlagzeilen durch zahlreiche und massive Sicherheitslücken

3 Für eine komplette Übersicht der Firefox-Marktanteile in Europa siehe *http://www.xitimonitor.com/etudes/equipement10.asp*.

4 Ab Firefox 1.5 wird es ein Quickmenü mit sicherheitsrelevanten Daten geben, das über die Tastenkombination Strg + Shift + Entf zu erreichen ist. Die Einstellungen, die im Folgenden beschrieben werden, können Sie dann dort vornehmen.

gemacht. Man darf jedoch nicht vergessen, dass Firefox noch sehr jung ist. In Zukunft kann man von dem Browser also noch viel erwarten. Die Anzahl an Sicherheitslücken ist kein besonders gutes Kriterium dafür, wie sicher eine Software im tatsächlichen Betrieb ist. Der Quell-Code von Firefox ist öffentlich verfügbar, und so lassen sich Fehler auch wesentlich schneller finden, melden aber auch ausnutzen. Die Mozilla-Community reagiert jedoch mit einer unglaublichen Geschwindigkeit auf diese Fehler und stellt Work-Arounds oder Updates zur Verfügung. Fehler im Internet Explorer bleiben dagegen oft über Monate hinweg bestehen und lassen den Angreifern damit genug Zeit zum Schreiben von Programmen, die genau diese Lücken ausnutzten.

Firefox läßt sich über so genannte *Extensions* beliebig erweitern und mit neuen Funktionen aufrüsten. Dies macht den Browser sehr flexibel. Auf der anderen Seite ist nicht gewiss, ob die Autoren der Erweiterungen die gleichen hohen Maßstäbe in Bezug auf Sicherheit anlegen wie das Mozilla-Team. Jede Erweiterung bringt also auch Risiken mit sich. Zudem müssen Sie sich anschließend nicht mehr nur um die Firefox-Updates kümmern, sondern auch nach solchen für jede einzelne Erweiterung suchen. Inzwischen bietet Firefox Ihnen die Möglichkeit, automatisch nach Updates (auch für die Erweiterungen) zu suchen.

Viele empfehlenswerte Links und Tipps zu Firefox finden sie unter *http://firefox.bric.de/index.php*.

Cookies

In Firefox lassen sich die Cookie-Optionen über EXTRAS → EINSTELLUNGEN... erreichen (siehe Abbildung 5-2). Sie befinden sich dort auf dem Reiter DATENSCHUTZ und müssen nun nur noch auf COOKIES klicken. Neben der Möglichkeit, Cookies ganz zu sperren, gibt es die Option NUR VON DER URSPRÜNGLICHEN WEBSITE. Mit dieser Option bestimmen Sie, dass nur der Server der eigentlichen Website und nicht auch die Server der Werbebanner Cookies auf Ihrem Rechner ablegen können (man spricht hier von Fremd-Cookies oder Third-Party-Cookies). Zudem gibt es die Möglichkeit einzustellen, wie lange die Cookies erhalten bleiben sollen und ob Sie Nachfragen von Firefox wünschen.

Viel interessanter sind jedoch die Optionen, die sich hinter den beiden Buttons AUSNAHMEN und COOKIES ANZEIGEN verbergen. Mit Hilfe des erstgenannten können Sie für einzelne Webseiten bestimmen, ob Cookies explizit erlaubt oder verboten werden sollen. Der zweite Knopf führt zu einer Auflistung aller derzeit gespeicherten Cookies. Dort können Sie sich deren Inhalt genau anschauen und die Cookies beliebig einzeln löschen. Zudem lässt sich festlegen, ob man einen einmal gelöschten Cookie in Zukunft generell ablehnen möchte. Diese Möglichkeit ist viel praktischer als das manuelle Setzen von Ausnahmen, da man zudem nur einen bestimmten unerwünschten Cookie verbietet und nicht alle von einem konkreten Server.

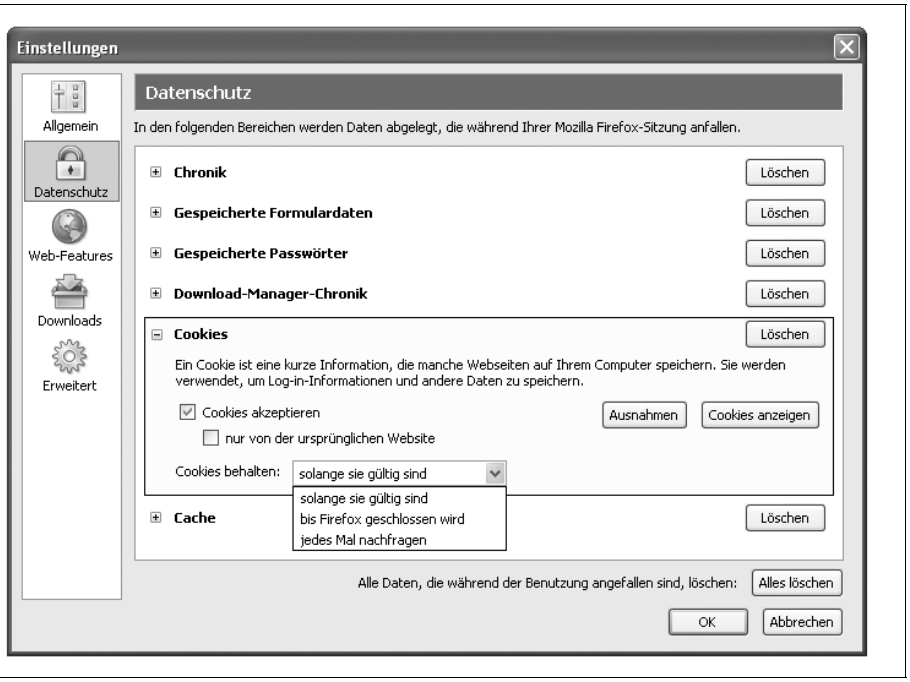

Abbildung 5-2: Das Dialogfeld Einstellungen in Firefox

ActiveX und Visual Basic Script

Firefox-Benutzer können beruhigt aufatmen, denn der Browser unterstützt weder ActiveX noch VBS in irgendeiner Form. Damit ist die größte Gefahr gebannt. Natürlich bedeutet der Verzicht auf ActiveX in gewisser Hinsicht auch einen Komfortverlust, da manche Webseiten ActiveX einsetzen, um erweiterte Funktionen anbieten zu können. Da aber immer mehr Verantwortliche einsehen, dass es unvernünftig ist, mehrere Millionen potenzieller Kunden auszuschließen, realisieren viele Anbieter ihre Webauftritte so, dass sie für die Mehrzahl der Browser komfortabel zu bedienen sind. Ein verstärkter Einsatz von Technologien wie Java-Applets wäre hier wünschenswert.

JavaScript und Java

Obwohl JavaScript und Java außer der Namensähnlichkeit kaum Gemeinsamkeiten aufweisen (siehe dazu Kapitel 4, *World Wide Web*), stehen sie im Konfigurationsmenü direkt nebeneinander. Deshalb wollen wir sie hier auch gemeinsam betrachten. JavaScript ist eine Erfindung der Firma Netscape. Aus diesem Grund ist der unterstützte Befehlsumfang von JavaScript in Firefox *vorbildlich*. Im Hinblick auf die Sicherheit ist vor allem interessant, dass man JavaScript nicht nur zentral an-

und ausschalten kann, sondern dass es ebenso möglich ist, gezielt bestimmte JavaScript-Funktionen zu deaktivieren. Die entsprechenden Buttons finden sich unter EXTRAS → EINSTELLUNGEN... → WEB-FEATURES. Per Klick auf ERWEITERT... gelangen Sie zu den einzelnen Funktionen. Die dortige Liste ist jedoch keineswegs vollständig; weitere Einstellungsmöglichkeiten zu JavaScript erreichen Sie, indem Sie **`about:config`** in die Adresszeile Ihres Browsers eingeben. Die vielen Optionen an dieser Stelle zu erläutern, ginge allerdings zu weit. Um im Dickicht dieser Optionen nicht den Überblick zu verlieren, finden Sie unter *http://www.firefox-browser.de/wiki/about:config* eine Einführung in die Arbeit mit dem Befehl `about:config`. Unter *http://www.firefox-browser.de/wiki/about:config_Einstellungen* finden Sie darüber hinaus eine Liste aller Optionen samt kurzer Erläuterung. Außerdem sei Ihnen das Buch *Firefox – Alles zum Kultbrowser* von Lars Schulten (O'Reilly 2005) ans Herz gelegt.

Cache, History und Passwort-Manager

Die Einstellungen für Cache und History (auch *Chronik* genannt) finden Sie ebenfalls unter EXTRAS → EINSTELLUNGEN... auf dem Reiter DATENSCHUTZ. Hier können Sie festlegen, wie groß der Cache sein soll, und diesen auch komplett leeren. Bezüglich der History gilt es zwischen der Chronik für die Adressleiste und der für den Download-Manager zu unterscheiden. Beide lassen sich getrennt voneinander löschen. Im Fall des Download-Managers ist es zudem möglich, die einzelnen Downloads direkt nach dem Herunterladen aus der Chronik zu entfernen.

Im Bereich DATENSCHUTZ befinden sich auch die Optionen für den Passwort-Manager. Prinzipiell raten wir davon ab, solche Manager zu benutzen – vor allem, wenn Sie nicht allein an Ihrem PC sitzen. Der Sinn eines solchen Managers ist es, die Passwörter, die Sie auf verschiedenen Webseiten angeben, zu speichern und bei Eingabe des Benutzernamens auf einer Webseite das dazugehörige Passwort automatisch zu ergänzen. Natürlich fragt Firefox bei jeder Seite nach, ob Sie das Passwort speichern möchten. Haben Sie sich jedoch einmal dafür entschieden, kann jeder Benutzer, der über den gleichen Windows-Account arbeitet wie Sie, diese Passwörter nutzen. Wenn Sie also nicht der alleinige Nutzer sind, sollten Sie Passwörter auf keinen Fall speichern.

Wenn Sie Ihren Rechner jedoch als einziger User nutzen und sich eine Gedächtnisstütze für Ihre Passwörter im Web wünschen, können Sie in Firefox ein so genanntes *Master-Passwort* festlegen. Damit schützen Sie alle von Ihnen hinterlegten Passwörter für Webseiten mit einer weiteren Kennung, die ein Mal pro Firefox-Sitzung abgefragt wird. Festlegen können Sie dieses Passwort über EXTRAS → EINSTELLUNGEN → DATENSCHUTZ → GESPEICHERTE PASSWÖRTER → MASTERPASSWORT... Natürlich bleibt auch hier ein Restrisiko, da Sie alle Ihre Web-Accounts einem einzigen Programm anvertrauen. Unserer Meinung nach ist dies jedoch ein guter Kompromiss zwischen Bedienbarkeit und Sicherheit. Letztendlich hängt es aber stark

davon ab, wie sicher Ihr Computer allgemein ist, wer daran arbeitet und wie sensibel die Account-Daten sind.

Popup-Blocker

Generell lohnt es sich, den Popup-Blocker zu aktivieren und einzelnen Seiten das Öffnen von Popup-Fenstern zu erlauben. Die dafür nötigen Einstellungen finden Sie über EXTRAS → EINSTELLUNGEN → WEB-FEATURES.

Internet Explorer

Um es gleich vorwegzunehmen: Der Internet Explorer ist, entgegen zahlreicher Behauptungen, kein schlechtes Produkt. So zeichnet er sich beispielsweise durch sein sehr stabiles Laufverhalten aus und stürzt entsprechend selten ab. Auf der anderen Seite muss man jedoch einräumen, dass er hoffnungslos veraltet und inzwischen technisch weit abgeschlagen ist. Dies gilt auch in Bezug auf die Sicherheit, bei der der Internet Explorer zurecht als Schlusslicht am Browsermarkt bezeichnet wird. Die bei der Drucklegung dieses Buches aktuelle Version 6 wird voraussichtlich im Laufe des ersten Quartals 2006 von Version 7 abgelößt, die nach fast vier Jahren Stillstand[5] (so lange ist die aktuelle Version bereits auf dem Markt) neue Funktionen und ein neues Sicherheitskonzept beinhalten wird. Durch die weite Verbreitung des Browsers (mehr als 80% Marktanteil) sind leider sehr viele Sicherheitslücken bekannt geworden. Dass sich das Schreiben eines Wurms oder Trojaners, der solche Lücken ausnutzt, bei einer solchen Marktdominanz besonders lohnt, ist selbstverständlich, und so tauchen oft schon wenige Stunden nach Bekanntgabe der Lücke erste Angriffstools auf. Zu der daraus resultierenden Verunsicherung trägt auch die nicht besonders transparente Firmenstrategie von Microsoft bei. Wie bereits beschrieben ist der Internet Explorer sehr eng an das Windows-Betriebssystem gekoppelt. Man kann sogar mittels Active Desktop Webseiten auf den Desktop legen, so dass diese als aktiver Hintergrund dienen und dort beispielsweise aktuelle Nachrichten erscheinen. Ebenfalls bedenklich ist die Verwendung der Programmiersprache Visual Basic Script und vor allem der ActiveX-Controls. Die JavaScript-Implementierung ist bewusst so gehalten, dass sie inkompatibel zu anderen Browsern ist, beschert Internetprogrammierern immer wieder Kopfzerbrechen und sorgt für zahlreiche Fehler bei der Webseitendarstellung.

Das zentrale Konfigurationstool finden Sie im Menü EXTRAS unter INTERNETOPTIONEN. Die hier getroffenen Sicherheitseinstellungen gelten leider für das E-Mail-Tool (Outlook Express) und den Browser gleichzeitig. Wichtig für uns sind erst einmal

5 Auch wenn vier Jahre im Internet eine sehr lange Zeit sind, hat Microsoft natürlich dennoch kleine Änderungen und Verbesserungen in die aktuelle Version eingebaut, vor allem aber viele Sicherheitslücken beseitigt.

nur die Registerkarten ALLGEMEIN, SICHERHEIT, DATENSCHUTZ UND ERWEITERT. Da auch der Internet Explorer über viele dutzend Optionen und verschachtelte Menüs verfügt, wollen wir uns hier nur auf einige relevante Grundkonfigurationen beschränken.

Die Registerkarte SICHERHEIT führt Sie zu einer Auswahl, in der Sie für vier verschiedene Zonen Sicherheitsstufen vergeben können. Bei diesen Zonen handelt es sich im Einzelnen um INTERNET, LOKALES INTRANET, VERTRAUENSWÜRDIGE SITES und EINGESCHRÄNKTE SITES. Prinzipiell sollte für alle Zonen die Sicherheitsstufe MITTEL oder HOCH eingestellt werden. In fast allen Fällen müssen Sie aber trotz des auf den ersten Blick bequemen Sicherheitsreglers selbst Hand anlegen. Da die Konfiguration hier nicht so trivial wie bei Firefox ist, wollen wir die im Firefox-Abschnitt eingeführte Aufteilung beiseite lassen und uns Stück für Stück durch die Vielfalt der Einstellungsmöglichkeiten arbeiten. Ein völlig abgesicherter Internet Explorer wird Ihnen jedoch wenig Spaß beim Surfen bereiten, so dass wir deshalb versuchen werden, einen guten Kompromiss zwischen Sicherheit und Komfort zu finden.

Kommen wir zunächst einmal zu den Sicherheitszonen: Die Internetzone beschreibt alle Webseiten außerhalb unseres lokalen Intranets, die weder in der Zone der vertrauenswürdigen noch in der der eingeschränkten Seiten stehen – kurz gesagt: alle Webseiten, bei denen Sie keine Spezialregelung wünschen. Die lokale Zone umfasst die Seiten in Ihrem eigenen Netzwerk. Das könnte beispielsweise eine betriebsinterne browsergestützte Applikation sein, jedoch auch eine bösartige Webseite, die auf einen lokalen Server geraten ist. Die Zone der vertrauenswürdigen Seiten beschreibt die Angebote im Internet, die sie per Hand als sicher eingestuft haben, die Zone der eingeschränkten Seiten hingegen solche, die Sie explizit als nicht vertrauenswürdig angegeben haben. Nun werden Sie sich fragen, warum es ratsam sein soll, trotz dieses Zonenmodells überall eine mittlere oder hohe Sicherheitsstufe einzustellen und noch dazu weitere Einstellungen per Hand vorzunehmen. Im Fall der eingeschränkten und der Internetzone dürfte dies ohnehin klar sein, denn hier ist das Gefahrenpotenzial am größten. Man darf sich zurecht, nicht nur beim Internet Explorer, fragen, wozu man Seiten, denen man nicht traut, überhaupt besuchen sollte. Es mag aber Situationen geben, in denen dies nötig ist. Im Fall der lokalen Zone ist es immer wieder zu Sicherheitslücken gekommen, wenn entweder tatsächlich lokal liegende Dokumente infiziert waren oder es Angreifern möglich war, den Internet Explorer auszutricksen und externe Seiten mit den Rechten der lokalen Zone auszuführen. Eine zu schwache Sicherheitseinstellung bei der lokalen (und möglicherweise auch vertrauenswürdigen) Zone kann daher zu ernsthaften Problemen führen und Ihr System in die Hände des Angreifers bringen. ActiveX-Komponenten sind einfach zu mächtige Werkzeuge, als dass man sie ohne Nachfragen und Restriktionen laufen lassen sollte. Die mittlere Zone ist, wenn man noch etwas per Hand nachhilft, jedoch wirklich als fairer Kompromiss zwischen Bedienbarkeit und Sicherheit zu bezeichnen. Je nach individuellem Gefahrenpotenzial müssen Sie die Einstellungen möglicherweise nochmals verschärfen, um wirklich auf der sicheren

Seite zu sein. Selbst dann, so haben unzählige Fälle in der Vergangenheit gezeigt, sind sie mit dem aktuellen Internet Explorer nicht wirklich sicher. Daher ist gerade bei diesem Produkt das regelmäßige Einspielen neuer Updates unverzichtbar.[6]

Kommen wir nun aber zur Konfiguration: In der Regel gibt es zu jedem Eintrag drei Auswahlmöglichkeiten: AKTIVIEREN, DEAKTIVIEREN und EINGABEAUFFORDERUNG. Letzteres bedeutet, dass der Browser jedes Mal nachfragt, wie er sich im konkreten Fall verhalten soll. Das ist zwar sehr informativ, da Sie dadurch ein gutes Gefühl dafür bekommen, wie oft und bei welchen Seiten eine bestimmte Technologie angewandt wird, bei vielen Einstellungen sind die aufspringenden Warnfenster aber eher nervtötend. Bedenken Sie zudem, dass einige Seiten mit aktiven Inhalten nicht mehr angezeigt werden können, wenn bestimmte Funktionen wie z. B. ActiveX deaktiviert sind. Wenn Sie also beim Surfen plötzlich vor weißen Seiten sitzen oder diese ein ungewöhnliches Verhalten aufweisen, sollten Sie versuchen, die eine oder andere Einstellung zu lockern, vorausgesetzt natürlich, die Seite liegt in der vertrauenswürdigen Zone.

Alle folgenden Einstellungen gelten für die auf mittlere oder hohe Sicherheit gestellte Internetzone und das Menü EXTRAS → INTERNETOPTIONEN → SICHERHEIT → STUFE ANPASSEN... (siehe Abbildung 5-3).

ActiveX-Steuerelemente und Plugins

Gerade in diesem Bereich gilt es zwischen Sicherheit und Nutzbarkeit zu entscheiden. Unsignierte ActiveX-Controls sollten grundsätzlich ein absolutes Tabu sein. Die vermeintlich sicheren Controls ebenfalls komplett zu deaktivieren, wirkt zwar wie eine sinnvolle Maßnahme (und wird daher auch von zahlreichen Experten empfohlen), führt aber in eine Sackgasse. Will man wirklich ein hohes Maß an Sicherheit und deaktiviert jegliche aktiven Komponenten, bleibt vom Internet Explorer nichts mehr übrig, was seinen Einsatz rechtfertigen würde. Jeder Benutzer, der auf ActiveX verzichten kann, sollte ohnehin zu einem anderen Browser wechseln.[7] Daher empfehlen wir hier für zahlreiche Einstellungen die Stufe EINGABEAUFFORDERUNG, die Ihnen ermöglicht, das Ausführen einer bestimmten ActiveX-Komponente jeweils vorher zu untersagen oder abzusegnen. Da viele Seiten kein ActiveX benutzen, sollten die Nachfragen des Browsers nicht so häufig sein, dass sie stören.

6 Es sei ein weiteres Mal betont, dass die Sicherheitsproblematik beim Internet Explorer deshalb so schwer wiegend ist und von der Benutzung abgeraten wird, weil der Browser einerseits per ActiveX-Controls Zugriff auf sehr mächtige Funktionen hat, und weil er zweitens so weit verbreitet ist. Sicherheitslücken und Programmierfehler im Allgemeinen sind keineswegs ein Problem, das nur Microsoft-Produkte betrifft!

7 Wir wollen die Internetwelt jedoch nicht zu schwarz-weiß malen: Es gibt durchaus Internetangebote, die sich (fast) nur über ActiveX-Controls umsetzen lassen und wertvolle Dienste leisten. Als Beispiel sei hier die Windows Update-Plattform genannt, die über das Web Ihre Software prüft und auf dem neuesten Stand hält. Es gibt sicherlich zahlreiche, teils richtige Einwände gegen diese Technologie, aber Microsoft begibt sich in diesem Bereich endlich auf den richtigen Weg.

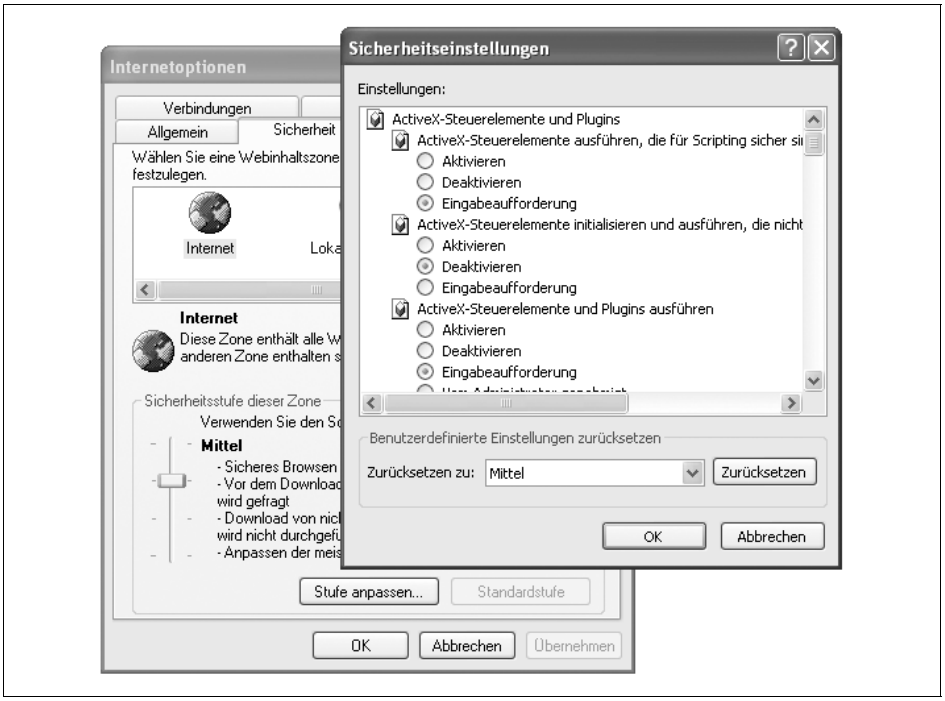

Abbildung 5-3: Das Dialogfeld Sicherheitseinstellungen im Internet Explorer

ACTIVEX-STEUERELEMENTE AUSFÜHREN, DIE FÜR SCRIPTING SICHER SIND
: Auch vermeintlich sichere ActiveX-Elemente können für Sie gefährlich werden. Sie sollten die Option also auf EINGABEAUFFORDERUNG stellen oder wenn nötig ganz deaktivieren. Letzteres kann vor allem sinnvoll sein, wenn eine neue Sicherheitslücke in der ActiveX-Behandlung gemeldet wurde, es aber noch kein Update von Microsoft gibt.

ACTIVEX-STEUERELEMENTE INITIALISIEREN UND AUSFÜHREN, DIE NICHT SICHER SIND
: Hier sollte unbedingt DEAKTIVIEREN eingestellt werden, da von diesen Elementen eine ernst zu nehmende Gefahr ausgeht.

ACTIVEX-STEUERELEMENTE UND PLUGINS AUSFÜHREN
: Auch bei dieser Option müssen Sie sich zwischen EINGABEAUFFORDERUNG und DEAKTIVIEREN entscheiden. Es gilt der bereits beschriebene Tipp, es zunächst einmal mit EINGABEAUFFORDERUNG ZU PROBIEREN.

BINÄR- UND SKRIPTVERHALTEN
: Diese Option ist mit dem Service Pack 2 von Windows XP neu hinzugekommen. Da es Viren gibt, die bei aktivierter Option Ihr System befallen können, sollten Sie diese Einstellung deaktivieren. Gelegentlich kann es daraufhin aber zu verschiedenen Fehlern und Debug-Meldungen kommen – in diesen Fällen müssen Sie die Option zwangsläufig aktiviert lassen.

DOWNLOAD VON SIGNIERTEN ACTIVEX-STEUERELEMENTEN
: Diese Option sollte ebenfalls per EINGABEAUFFORDERUNG gesichert oder sogar ganz deaktiviert werden.

DOWNLOAD VON UNSIGNIERTEN ACTIVEX-STEUERELEMENTEN
: Deaktivieren Sie diese Option. Unsignierte Elemente sind nicht vertrauenswürdig.

Benutzerauthentifizierung

In diesem Abschnitt könnten Sie die Standardoption belassen, es wäre jedoch besser, auf NACH BENUTZERNAME UND KENNWORT FRAGEN zu schalten. Bei höheren Sicherheitsanforderungen wird teilweise empfohlen, auf ANONYME ANMELDUNG umzustellen. Dies wird jedoch zu Fehlern führen und sollte vermieden werden, schließlich ist so der Zugriff auf passwortgeschützte Seiten und Bereiche (Verzeichnisse) unmöglich.

Download

Bis auf den *Schriftart-Download* können Sie die drei Einstellungen so belassen, wie sie sind. Das Sperren des Datei-Downloads mag bei öffentlich aufgestellen PCs sinnvoll sein, eignet sich aber nicht für den privaten PC, da Sie anschließend keinerlei Dateien (etwa Treiberupdates) mehr aus dem Internet laden können.

SCHRIFTART-DOWNLOAD
: Die Art der gewählten Schrift hat im Prinzip keinen Einfluss auf die Funktion einer Internetseite. Wenn Sie diese Option deaktivieren, kann es vorkommen, dass einige Seiten nicht mehr den Designansprüchen des Betreibers entsprechen, dafür ersparen Sie Ihrem Betriebssystem eine weitere Schriftart (wovon Sie ohnehin schon mehr als nötig besitzen). Um von Fall zu Fall unterscheiden zu können, sollte man hier EINGABEAUFFORDERUNG wählen.

Scripting

ACTIVE SCRIPTING
: Diese Einstellung gilt für Visual Basic Script und für JavaScript. Eine vollständige Deaktivierung ist zwar das einzig Sichere, Sie büßen damit jedoch viel Komfort ein. Versuchen Sie es testweise zunächst mit EINGABEAUFFORDERUNG. Leider kann es dann vorkommen, dass Sie kaum noch zum eigentlichen Surfen kommen, weil Sie dauernd mit dem Wegklicken der Warnmeldungen beschäftigt sind. Gute Webdesigner benutzen Skriptsprachen eigentlich nur für technische und gestalterische Raffinessen und nicht für die essentiellen Dienste, die auf der Webseite angeboten werden. Da das Web aber zunehmend hohen Komfort- und Designansprüchen standhalten muss und Skripte daher eher häufiger

als seltener werden, müssen Sie früher oder später auf AKTIVIEREN umschwenken.

EINFÜGEOPERATIONEN ÜBER EIN SKRIPT ZULASSEN
: Auch hier müssen Sie sich wieder zwischen EINGABEAUFFORDERUNG und DEAKTIVIEREN entscheiden. Skripten wird es durch diese Operationen möglich, die Zwischenablage auszulesen, was unter Umständen ein Sicherheitsrisiko sein könnte. Meine persönliche Empfehlung wäre die Einstellung EINGABEAUFFORDERUNG.

SCRIPTING VON JAVA-APPLETS
: Wählen Sie auch hier EINGABEAUFFORDERUNG ODER DEAKTIVIEREN, WENN SIE AUF HOHE SICHERHEIT WERT LEGEN (MÜSSEN).

Java (»Microsoft VM«)

Ob diese Option überhaupt auftaucht, hängt von der Version Ihres Explorers ab. Microsoft möchte seine eigenen Programmiersprachen durchsetzen und unterstützt Java daher nicht mehr von Hause aus.[8]

JAVA-EINSTELLUNGEN
: Hier sollten Sie die Einstellung HOHE SICHERHEIT oder gar DEAKTIVIEREN wählen, je nachdem, wie oft Sie Applets benötigen.

Verschiedenes

AUF DATENQUELLEN ÜBER DOMÄNENGRENZEN HINWEG ZUGREIFEN
: Deaktivieren Sie diese Option sicherheitshalber. Sie erlaubt es dem angesprochenen Webserver, Daten von anderen Servern in Ihren Browser zu laden. Meistens handelt es sich dabei um harmlose Vorgänge, aber in jedem Fall verlieren Sie die Übersicht darüber, woher die Daten eigentlich kommen.

DATEIEN BASIEREND AUF DEM INHALT UND NICHT DER DATEIERWEITERUNG ÖFFNEN
: Diese neue Option ist sehr wichtig, da sie Angriffe über falsche oder doppelte Dateierweiterungen verhindert, und sollte daher unbedingt aktiviert bleiben.

DAUERHAFTIGKEIT VON BENUTZERDATEN
: Diese Option kann und sollte aus Komfortgründen aktiviert bleiben

GEMISCHTE INHALTE ANZEIGEN
: Wählen Sie hier EINGABEAUFFORDERUNG, denn DEAKTIVEREN würde zwar die Sicherheit erhöhen, wäre aber wenig sinnvoll.

8 Diese traurige Entwicklung beruht auf einem weiteren Schachzug des Monopolisten, um die plattformunabhängige Sprache Java zu untergraben. Sie können die Virtual Machine für den Internet Explorer jedoch von Hand nachinstallieren.

INSTALLATION VON DESKTOPOBJEKTEN

Diese Funktion kann ebenfalls deaktiviert werden, ohne dass der Browser an Komfort verliert. Hier würde sich aber auch die Einstellung EINGABEAUFFORDERUNG anbieten, da sie Ihnen mehr Einflussmöglichkeiten bietet, ohne dass es in diesem Fall zu einem Komfortverlust durch häufige Nachfragen kommt.

KEINE AUFFORDERUNG ZUR CLIENTZERTIFIKATSAUSWAHL, WENN KEIN ODER NUR EIN ZERTIFIKAT VORHANDEN IST

Diese Option sollte, wie in den Standardeinstellungen bereits gesetzt, deaktiviert bleiben.

META REFRESH ZULASSEN

Diese Option sollte aktiviert bleiben.

POPUP-BLOCKER VERWENDEN

Der Popup-Blocker erweist sich zwar auf zahlreichen Seiten als hinderlich (z.B. beim Firstgate-Zahlungssystem oder bei Bankapplikationen), ist aber grundsätzlich sinnvoll, so dass er aktiviert bleiben sollte. Sie können Popups dennoch von Fall zu Fall zulassen oder für bestimmte Seiten komplett erlauben. Den erweiterten Popup-Manager finden Sie unter EXTRAS → INTERNETOPTIONEN → DATENSCHUTZ → EINSTELLUNGEN...

PROGRAMME UND DATEIEN IN EINEM IFRAME STARTEN

Mit dieser Funktion ist es möglich, Dateien verschiedenster Herkunft in unterschiedlichen Frames (Teilfenstern) zu laden. Dadurch geht für den Benutzer aber die Transparenz verloren, da es eventuell schwer nachzuvollziehen ist, auf welcher Internetseite er sich zurzeit befindet. Sie sollten dies nicht ohne Nachfrage zulassen.

SCRIPT-INITIIERTE FENSTER OHNE GRÖSSEN- BZW. POSITIONSEINSCHRÄNKUNGEN ZULASSEN

Diese Option ist zurecht deaktiviert und sollte es auch bleiben.

SCRIPTING DES INTERNET EXPLORER-WEBBROWSERSTEUERELEMENTS ZULASSEN

Auch hier ist bei mittlerer Sicherheitsstufe bereits die richtige Option, DEAKTIVIEREN, gewählt.

UNVERSCHLÜSSELTE FORMULARDATEN ÜBERMITTELN

Da wir bisher viele Funktion deaktiviert haben, gehen Sie sicherlich davon aus, dass wir unverschlüsselte Formulardaten erst recht nicht erlauben sollten. Eigentlich haben Sie damit recht, denn unverschlüsselte Daten können von Angreifern aus dem Datenstrom im Klartext ausgelesen werden. Leider funktionieren dann viele Webseiten nicht mehr, beispielsweise können Sie keine Suchmaschinen mehr abfragen oder Formulare ausfüllen. Sie müssen diese Funktion deshalb aktivieren oder zumindest auf EINGABEAUFFORDERUNG setzen. Da Sie die ständigen Nachfragen aber spätestens nach einem Tag gedankenlos wegklicken werden, empfiehlt es sich eventuell, die Option aktiviert zu lassen.

VERWENDUNG EINGESCHRÄNKTER PROTOKOLLE MIT AKTIVEN INHALTEN FÜR WEBSEITEN ZULASSEN

Belassen Sie auch hier die Einstellung auf EINGABEAUFFORDERUNG.

WEBSITES, DIE SICH IN WEBINHALTSZONEN NIEDRIGER BERECHTIGUNG BEFINDEN, KÖNNEN IN DIESE ZONE NAVIGIEREN

Hier sollten Sie von AKTIVIEREN zu EINGABEAUFFORDERUNG wechseln.

ZIEHEN UND ABLEGEN ODER KOPIEREN UND EINFÜGEN VON DATEIEN

Mittels dieser Funktion wird es dem Server ermöglicht, automatisch Dateien auf dem System des Surfers abzulegen. Lassen Sie den Browser vor solchen Aktionen grundsätzlich nachfragen.

ZUGRIFFSRECHTE FÜR SOFTWARECHANNEL

Wenn Sie einen so genannten Softwarechannel abonniert haben, wird von dort aus Software direkt auf Ihr System heruntergeladen. Da dies jedoch im Hintergrund geschieht und nicht sichergestellt werden kann, dass die Programme keine Viren oder Trojaner enthalten, sollten Sie hier unbedingt die höchste Sicherheitsstufe einstellen.

CACHE, HISTORY UND ADRESSLEISTE

Verlassen Sie die Registerkarte SICHERHEIT und wechseln zu ALLGEMEIN. Den Verlauf (History) können Sie mittels VERLAUF LEEREN löschen. Ansonsten wird der Browser aufzeichnen, welche Seiten Sie besucht haben. Sind Sie der einzige Benutzer des Computers, brauchen Sie den Verlauf jedoch nicht zu löschen. Den Cache können Sie über die Schaltfläche DATEIEN LÖSCHEN leeren. Achten Sie jedoch darauf, dabei auch die Option ALLE OFFLINEINHALTE LÖSCHEN zu aktivieren.

COOKIES

Die Cookie-Einstellungen erreichen Sie über den Reiter DATENSCHUTZ. Wie bereits besprochen, ist der Umgang mit Cookies eine Frage der persönlichen Präferenzen. Wir zeigen hier eine sichere Einstellung (siehe Abbildung 5-4) – inwieweit Sie diesem Vorschlag folgen, bleibt Ihnen überlassen.

Klicken Sie also bei den Datenschutzeinstellungen auf ERWEITERT und heben die automatische Cookiebehandlung auf. Anschließend sperren Sie sowohl Cookies von Erst- als auch Drittanbietern, erlauben aber Session-Cookies. Dies sollte ein ausreichend gutes Verhältnis von Sicherheit zu Komfort sein, bestätigen Sie Ihre Eingaben mit OK. Einzelnen Seiten können Sie gesondert andere Rechte zuordnen, indem Sie auf dem Reiter DATENSCHUTZ zurückkehren und dort auf den Button SITES... klicken. Im folgenden Dialogfenster können Sie die URLs der Seite angeben, die Sie sperren bzw. zulassen wollen.

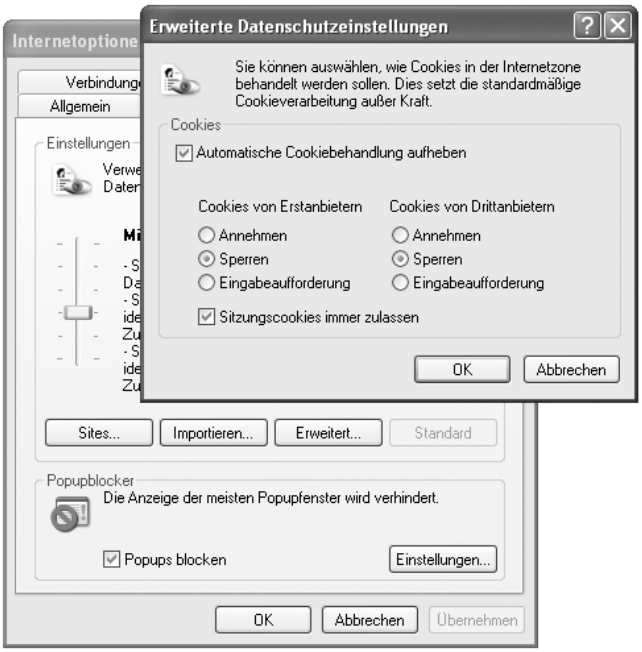

Abbildung 5-4: Cookie-Einstellungen im Internet Explorer

Weitere Optionen

Auf der Registerkarte ERWEITERT sollten Sie die Funktionen AUF ZURÜCKGEZOGENE SERVERZERTIFIKATE ÜBERPRÜFEN (NEUSTART ERFORDERLICH) im Bereich SICHERHEIT aktivieren. Zuletzt können Sie noch einen Blick auf den Reiter INHALTE werfen. Dort finden Sie die Einstellungen für die Autovervollständigung von Formularen und Kennwörtern. Wenn Sie diese Funktionen nutzen wollen, sollten Sie jedoch zumindest das Nachfragen bei Benutzerdaten aktiviert lassen.

Allgemeine Sicherheitshinweise

Wie Sie gesehen haben, kann man den Internet Explorer bis ins Detail gegen Sicherheitsrisiken absichern. Dies wirkt zwar auf den ersten Blick elegant, überfordert die meisten Benutzer jedoch. Zudem verändern sich die Menüs und Einträge natürlich von Update zu Update. Generell sollten Sie jede Funktion, deren Bedeutung und Auswirkung Sie nicht verstehen, auf EINGABEAUFFORDERUNG stellen. Mit der neuen Version Internet Explorer 7 mag sich einiges ändern (hoffentlich zum Guten), bis dahin sei aber vom intensiven Gebrauch des Internet Explorers abgeraten.

Opera

Der aus Norwegen stammende Opera-Browser ist seit der Version 8.5 auch ohne Werbeeinblendungen völlig kostenlos. Damit erhoffen sich die Entwickler den Marktanteil dieses herausragenden Produktes weiter zu steigern. Aktuell dürfte dieser bei unter 5% liegen, so dass Opera die dritte Position hinter dem Internet Explorer und der Mozilla-Familie einnimmt. Opera zeichnet sich seit jeher durch seine Schlankheit sowie die Geschwindigkeit beim Laden von Websites aus. Zudem ist Opera sowohl Firefox also auch dem Internet Explorer in punkto Geschwindigkeit, Funktionsumfang und vor allem Innovation überlegen: Neben zahlreichen nützlichen Funktionen, wie etwa *tabbed browsing*, sollte das Zoomen nicht unerwähnt bleiben, mit dem man eine Webseite oder ein Bild um bis zu 400% vergrößern oder aber auch stark verkleinern kann. Erfreulich sind auch das funktionelle Design ohne unnötige Schnörkel und die *mouse gestures*, mit denen man zahlreiche Funktionen mittels einzelner Mausbewegungen ausführen kann. Aus Sicherheitsperspektive ist vor allem das Schnellmenü interessant, mit dem Sie über einen Druck auf die F12-Taste alle wesentlichen Funktionen auf einen Blick parat haben.

Früher hatte Opera zahlreiche Probleme mit Frames und JavaScript, dies ist aber spätestens seit der Version 7 Geschichte. ActiveX, VBS und zahlreiche Plugins werden allerdings nicht unterstützt. Aufgrund der fehlenden Werbung ist der Opera-Browser zurzeit eher noch ein Geheimtipp, gewinnt aber zunehmend an Bedeutung bei anspruchsvollen Benutzern. Opera-spezifische Sicherheitsmängel sind zurzeit nicht bekannt. In der Vergangenheit (auch 2005) hat es jedoch immer wieder kleinere und größere Probleme gegeben. Insgesamt ist Opera aber der sicherste Browser, wenn man die Anzahl der Lücken und die Geschwindigkeit, mit der diese beseitigt werden, als Maßstab nimmt. Herunterladen können Sie Opera (auch in deutscher Version) unter *http://www.opera.com*, es ist für Windows, Linux und fast alle weiteren gängigen und exotischeren Betriebssysteme wie z.B. MacOS, BeOS und OS/2 verfügbar. Den derzeit größten Erfolg feiert Opera aber wohl im Handy- und Smartphone-Markt.

Das zentrale Opera-Konfigurationstool für die Sicherheitseinstellungen (siehe Abbildung 5-5) finden Sie im Menü EXTRAS unter EINSTELLUNGEN ODER PER SCHNELLZUGRIFF ÜBER DIE BEREITS GENANNTE F12-TASTE. Im Gegensatz zu den anderen Browsern bietet Opera über den HILFE-Button im Einstellungsmenü zahlreiche detaillierte Tipps und Informationen.

Privatsphäre

Die für Ihre Privatsphäre interessanten Einstellungen erreichen Sie im Einstellungsmenü über den Reiter ERWEITERT und dort unter VERLAUF, COOKIES, SICHERHEIT und NETZWERK. Referrer-Informationen und Cookies können Sie zudem über F12 an- und ausschalten.

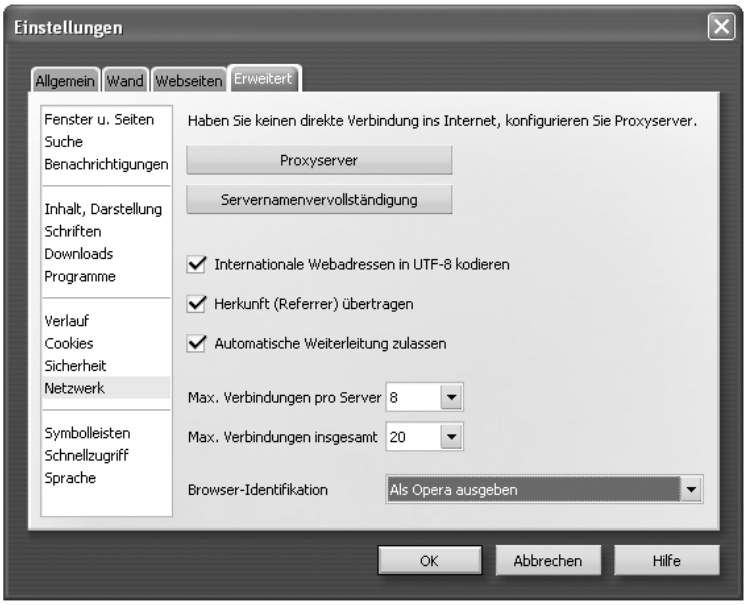

Abbildung 5-5: Das Dialogfeld Einstellungen in Opera

COOKIES

Zum Thema Cookies hält Opera besonders viele Konfigurationsoptionen bereit. Wie auch die anderen Browser bietet Opera Ihnen an, vor jedem Cookie zu fragen, ob Sie ihn akzeptieren wollen. Darüber hinaus gibt es die Möglichkeit, Cookies nur von bestimmten Seiten zu erlauben, die Sie in der Serververwaltung (COOKIES VERWALTEN) festlegen können. Da die daraus resultierende Liste ziemlich lang werden dürfte, erlaubt die Maske auch die Eingabe von Domains, aus denen Cookies nicht akzeptiert werden dürfen. Alle anderen Domains können dann weiterhin Cookies setzen. Zusätzlich können Sie Opera anweisen, akzeptierte Cookies nach dem Schließen des Browsers zu löschen. Dies ist ganz besonders nützlich, wenn Sie einen Cookie zur korrekten Anzeige der Seite zulassen müssen, ohne ihn auf lange Sicht behalten zu wollen. Aktivieren Sie dazu einfach die Option NEUE COOKIES IMMER BEIM BEENDEN LÖSCHEN. Zudem können Sie sich jeden einzelnen Cookie über die Serververwaltung anzeigen lassen. Die Cookies sind dort nach Servern sehr übersichtlich sortiert und lassen sich einzeln auswählen und in einer sehr übersichtlichen Maske anzeigen (siehe Abbildung 5-6). Darüber hinaus ist es möglich, nach Servern in einer Suchmaske zu suchen und Cookies sogar gezielt zu manipulieren. So kann man beispielsweise das Gültigkeitsdatum oder auch einzelne Wertepaare, die der Server gesetzt hat, verändern.

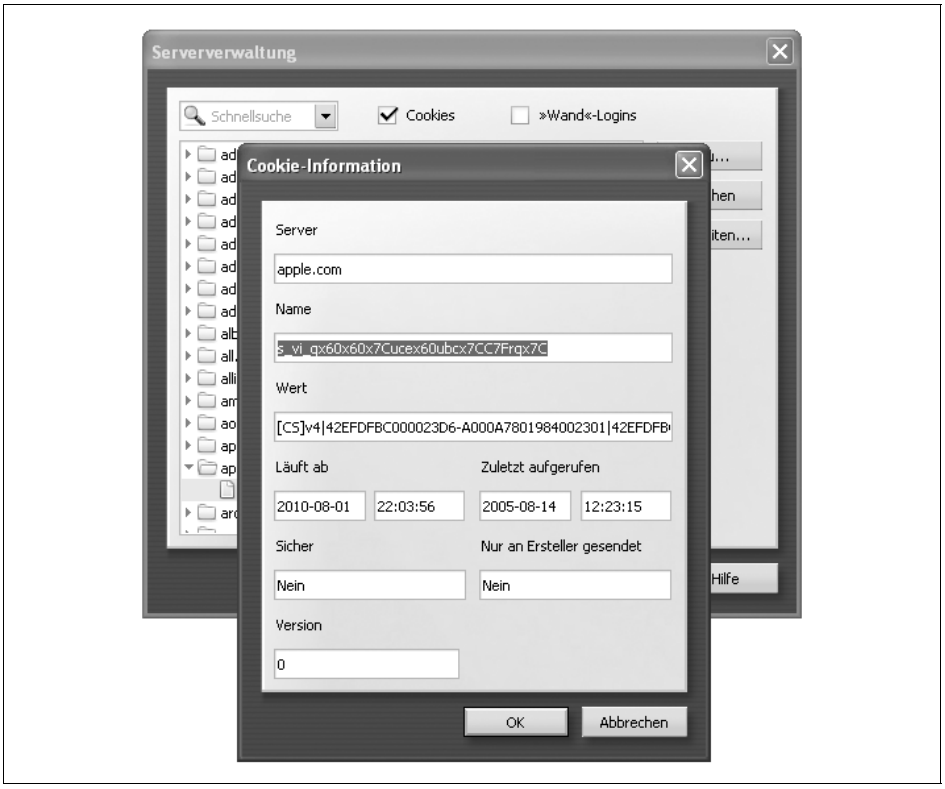

Abbildung 5-6: Die Opera-Serververwaltung mit einem geöffneten Cookie von apple.com

CACHE, HISTORY UND ADRESSLEISTE
: Unter VERLAUF finden Sie wiederum eine Vielzahl möglicher Konfigurationsoptionen. Die dort standardmäßig gesetzten Einstellungen sind sinnvoll und bedürfen eigentlich keiner Änderungen. Sollten Sie nicht der alleinige Benutzer des Computers sein, ist es aber ratsam, die History und den Cache komplett abzuschalten oder zumindest regelmäßig zu löschen.

PASSWÖRTER UND FORMULARE
: Über den Reiter WAND können Sie ein Formularprofil anlegen und die zu speichernden Passwörter über die Serververwaltung handhaben. Über den Reiter ERWEITERT und den Abschnitt SICHERHEIT ist es zudem möglich, wie bei Firefox ein Master-Passwort zu setzen. Zusätzlich (um tatsächlich die Wand-Passwörter sowie diejenigen für E-Mail und News zu schützen) muss noch der Haken bei ALS MASTERPASSWORT FÜR E-MAIL UND WAND VERWENDEN gesetzt werden.

HERKUNFT ÜBERTRAGEN
: Was die meisten Nutzer nicht ahnen, ist im Web längst zum üblichen Vorgehen geworden: Die von Ihnen besuchte Webseite ist in der Lage herauszufinden, auf welcher Seite Sie zuletzt waren, sofern Sie über einen Link von einer Seite zur an-

deren gelangt sind. Tatsächlich macht das für viele Webseiten durchaus Sinn und ist vor allem auch für Rabattsysteme und Statistiken interessant. Für Sie als Kunde mag so ein Vorgehen jedoch auch Probleme mit sich bringen, schließlich könnte man auch argumentieren, dass diese Information zu Ihren persönlichen Daten gehört und der Betreiber einer Webseite nicht wissen muss, wo Sie sich sonst noch aufhalten. Daher können Sie Opera anweisen, diese Information zu unterdrücken. Dazu benutzen Sie wahlweise die F12-Taste oder den Haken HERKUNFT (REFERRER) ÜBERTRAGEN im Abschnitt NETZWERK des Reiters ERWEITERT.

Skriptsprachen, Plugins und Popup-Fenster

Im Abschnitt INHALT, DARSTELLUNG des Reiters ERWEITERT finden sich überraschenderweise die Einstellungen zu Java, JavaScript und den Plugins. ActiveX wird von Opera nicht unterstützt.

JAVASCRIPT UND JAVA
: Beide Sprachen können Sie in der Maske KOMPLETT deaktivieren. Alternativ dazu können Sie im Fall von JavaScript (unter JAVASCRIPT-OPTIONEN), ähnlich wie bei Firefox, einzelne JavaScript-Befehle an- und ausschalten. Ein Zonenmodell und/oder verschiedene Sicherheitsstufen bietet Opera leider nicht an.

PLUGINS
: Über eine weitere Checkbox kann zudem die Plugin-Unterstützung deaktiviert werden. Anschließend können Sie jedoch keine erweiterten Inhalte wie etwa Flash-Clips oder eingebundene Musikstücke anschauen bzw. anhören.

POPUP-FENSTER
: Per Druck auf F12 oder über den Reiter ALLGEMEIN können Sie den Popup-Blocker deaktivieren und konfigurieren. Hier sollte UNERWÜNSCHTE POPUPS BLOCKIEREN gewählt sein.

Weitere Optionen

Leider vergessen Webdesigner häufig, dass der Sinn einer Internetseite meist ein möglichst großer Informationsgehalt ist und nicht, die neuesten technischen Spielereien auszuprobieren. Der große Monopolist Microsoft ist zudem nicht daran interessiert, zu anderen Produkten kompatibel zu sein, und benutzt daher verschiedene Implementierungen von Skriptsprachen und HTML-Befehlen. Diese beiden Tatsachen bewirken, dass Webseiten oft versuchen, den Typ des Browsers zu ermitteln, um ihm eine passende Version der Seite zu bieten. Stoßen sie dabei nicht auf den Internet Explorer oder Firefox bzw. Netscape, sperren sie den fremden Browser häufig einfach aus. Um dieses Problem zu umgehen, kann sich Opera als einer dieser Browser tarnen. Dadurch kann man zwar bequem alle Seiten betrachten, wirkt aber dem wünschenswerten Umdenken der Webdesigner entgegen. Die Webmaster

und Designer sehen in Ihren Statistiken dann nämlich keine Opera-Browser, sondern nur die beiden großen Rivalen. Wenn Sie deshalb der Meinung sind, Opera sollte sich auch als er selbst zu erkennen geben, können Sie dies im Reiter ERWEITERT im Abschnitt NETZWERK (BROWSER-IDENTIFIKATION) einstellen. Inzwischen sollte dies bei den meisten Webseiten nicht mehr zu Schwierigkeiten in der Darstellung führen, ist dabei aber ein wichtiges Zeichen an die Web-Community.

Allgemeine Sicherheitshinweise

Wie zu Anfang bereits beschrieben, ist natürlich auch Opera nicht frei von Fehlern, er gilt jedoch zurecht als der zurzeit sicherster und fortschrittlichster Browser. Das liegt zu einem gewissen Teil aber auch daran, dass dieser Browser wegen seiner geringeren Verbreitung für Cracker wenig interessant ist. Es wird sich kaum jemand die Mühe machen, z.B. einen E-Mail-Virus speziell für das in Opera eingebundene Mailtool zu schreiben.[9]

Browserkonfiguration prüfen

Zur Überprüfung der Sicherheitskonfiguration Ihres Browsers ist die Webseite der Zeitschrift *c't* unter *http://www.heise.de/security/dienste/browsercheck/* zu empfehlen. Dort finden Sie neben interessanten Informationen zur Browsersicherheit auch die Beschreibung einiger ausgewählter Sicherheitslücken, anhand derer Sie nachvollziehen können, wie sicher Sie sich zurzeit durch das Internet bewegen. Besonders aufschlussreich ist auch hier die Vorher-Nachher-Analyse, um zu sehen, wie sich bestimmte Konfigurationsänderungen auf Ihre Sicherheit auswirken. In Kapitel 12, *Firewalls und erweiterte Sicherheitssysteme*, werden wir noch weitere Sicherheitsmaßnahmen vorstellen, deren Wirksamkeit Sie anschließend auf dieser Webseite ausprobieren können. Sehr eindrucksvoll und daher empfehlenswert ist ein Vorher-Nachher-Test mit einem unkonfigurierten Internet Explorer.

Übrigens sei dringend und nachdrücklich davon abgeraten, solche Tests auf vermeintlichen Sicherheits- oder gar Hackerseiten zu durchlaufen (erst recht nicht, wenn man dort zunächst aufgefordert wird, den Sicherheitslevel seines Browser herunterzuschrauben). Angreifer machen sich regelmäßig einen Spaß daraus, Seiten ins Netz zu laden, die angeblich völlig harmlose Tests von Sicherheitslücken erlauben. Solche Lücken gestatten oft genug das Lesen und Schreiben von Dateien auf Ihre lokale Festplatte. Sie sollten sich daher sehr genau überlegen, wessen Testdatei auf diese Weise am Ende auf Ihrer Festplatte landet. Natürlich gibt es auch eine Vielzahl seriöser Seiten und Tests, ein kritischer Blick ist aber Pflicht.

9 Das schließt natürlich nicht aus, dass es einmal solche Viren und Angriffswerkzeuge geben mag.