7 schockierende Wahrheiten über Windows

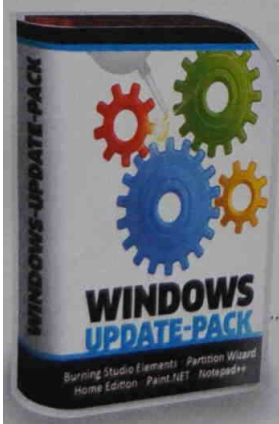
Der große Exklusiv-Report über Datenlecks, Echtheitsprüfung, Windows-7-Sicherheit ... ► 34

Ihr Rechner als

7 schockierende Wahrheiten über Windows

Ein tiefer Blick auf die hässliche Seite von Windows deckt Probleme auf, die Microsoft selbst erzeugt hat. Ihre Lösung bleibt Sache des Users

VON MARKUS MANDAU



AUF DVD

Mit unseren Tools wechseln Sie die ungenügenden Windows-Tools aus und beseitigen einige der wichtigsten Systemschwächen (CHIP-Code Wahrwin).

Microsoft mutet den Kunden mit Windows ganz schön viel zu. Bekannte Probleme wie Abstürze und Sicherheitslecks haben sich mit der Version 7 zwar gebessert, doch nach wie vor trauen User ihrem Windows nur bedingt. Kein Wunder, denn schließlich gehört ihnen das System nicht, die Lizenz erteilt nur ein Nutzungsrecht, das von Microsoft regelmäßig überprüft wird (siehe ► S. 36). Hinzu kommen die vielen Bugs (siehe Grafik rechts), mit denen die User häufig konfrontiert und manchmal allein gelassen werden. Wir zeigen die schlimmsten Zumutungen, die Microsoft seinem Betriebssystem – und damit Ihnen – antut und sagen, wie Sie die gröbsten Schnitzer beseitigen.

RÜCKSICHTSLOS

XP löscht Daten von Vista und Win 7

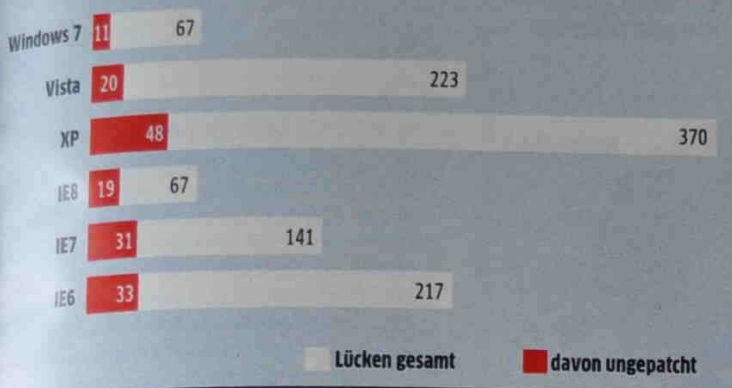
Wer Vista oder Windows 7 parallel zu XP installiert, muss aufpassen. Denn ohne Eingriff des Users funktioniert die Systemsicherung in Vista und Windows 7 nicht mehr. Dass XP beim Hochfahren die Wiederherstellungspunkte der neuen Versionen überschreibt, ist seit der Einführung von Vista vor über vier Jahren bekannt. Doch statt nachzubessern, setzt Microsoft noch einen drauf: Die Löschung betrifft in Windows 7 auch die Dateisicherung mit den Backups der älteren Dateiversionen.

Microsoft hat mit Vista die Systemsicherung grundlegend überarbeitet und speichert die Sicherungsdaten in Schattenkopien. Die sind mit dem Treiber volsnap.sys verknüpft, über den Windows die Partitionen einbindet und mountet. Liest XP die Laufwerke über seinen Volsnap-Treiber ein, erkennt es die Datensicherungspunkte nicht und überschreibt sie einfach.

Der Clou: Microsoft sagt selbst, dass ein Fix zu aufwendig ist, würde dies doch bedeuten, die Technik der Schattenkopien in XP einzuführen. Stattdessen empfiehlt der entsprechende Technet-Artikel, den Datenträger mit Vista beziehungsweise Windows 7 abzuklemmen, bevor XP hochfährt. Nur →

WINDOWS-BUGS: NICHT GEPATCHT SEIT 2002

Microsoft schließt nicht alle bekannten Windows- und IE-Lücken. Manche sind schon seit mehr als acht Jahren offen



KERNEL-CRASH: AUSFÄLLE DER SYSTEMKOMPONENTEN

Welche Kernel-Dateien von Windows besonders anfällig sind, zeigt die Liste der ab XP aufgetretenen Kernel-Bugs

Name	Funktion	Anzahl der Fehler
win32k.sys	Stellt Kernel-Funktionen für die Windows-API zur Verfügung, darunter die Anzeige der grafischen Oberfläche	18
ntdll.dll	Zentrale Schnittstelle für Komponenten, die im User-Mode – also weniger stark abgesichert – auf der CPU laufen	7
lsass.exe	Der Local Security Authentication Server überprüft die Gültigkeit der Benutzeranmeldung	7
csrss.exe	Der Client Server Runtime Process ist unter anderem dafür zuständig, Threads anzulegen und zu beenden	6
gdi32.dll	Das Graphics Device Interface ist für alle Windows-Anwendungen die zentrale Schnittstelle zur Grafikkarte	5

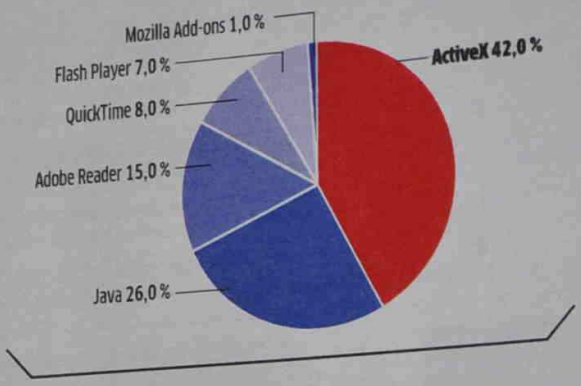
ist das keine Lösung, wenn die Systeme auf einer Platte sind.

Wir empfehlen, die Systempartitionen von Vista und Windows 7 vor XP zu verstecken. Dazu müssen Sie bei XP in der Registry unter »HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices« den Schlüssel »Offline« anlegen. Darin erzeugen Sie den DWORD-Unterschlüssel »\DosDevices\D:« und geben ihm den Wert »1«. Wobei „D:" für das Laufwerk steht, auf dem sich laut Explorer das neuere Windows befindet.

Eine andere Inkompatibilität zwischen XP und seinen Nachfolgern: Das ältere System startet vom Sektor 63 seine NTFS-Platte, Vista und Windows 7 von 1024. Erzeugen Sie in XP oder mit einem alten Partitionsmanager eine neue Partition, so sind alle zuvor mit Vista oder Windows 7 angelegten Laufwerke verschwunden. Die Lösung von Microsoft: Dann nehmen Sie eben nicht XP, um Partitionen anzulegen. Unsere Antwort finden Sie auf der Heft-DVD: Den Partition Wizard, er ist kompatibel mit Vista und Windows 7.

BROWSERLÜCKEN

Die Windows-Schnittstelle ActiveX verursacht fast die Hälfte aller Schwachstellen in Browser-Plug-ins



UNSICHER

Verwundbare Systemkomponenten

Der Kernel gilt als besonders geschützter Teil von Windows. Läuft hier etwas schief, ist oft das ganze System in Gefahr. Umso erstaunlicher, dass sich mit nur einem geänderten Registrywert das Kernel-Modul win32k.sys kompromittieren lässt. Ein Angreifer kann dadurch auch unter Windows 7 und bei aktivierter User Account Control die höchsten Systemrechte erlangen. Diese Lücke wurde erst Ende November 2010 entdeckt – und ist bis heute nicht gefixt.

Der ursprüngliche Fehler liegt im Systemmodul RtlQueryRegistryValues, das die Tabelle der Registrywerte im RAM verwaltet. Den Werten ist ein Eintrag über die Größe des Arbeitsspeicherbereichs zugeordnet, der etwa als DWORD-Zeichenfolge vorliegt. Lässt sich aber der Typ eines Registry-Eintrags auch mit geringeren Rechten in einen Binärwert umwandeln, ändert sich die Größe des mit dem Eintrag verknüpften Arbeitsspeicherbereichs. Die Folge ist ein Pufferüberlauf. Hacker haben für die win32k.sys genau einen solchen Eintrag aufgespürt. Ein Beispiel inklusive Code findet sich auf der Webseite von The Code Project – allerdings ziemlich versteckt (**http://68.233.235.195/kmax/security-uac.aspx.htm**).

Der Klassiker unter den unsicheren Systemkomponenten hat aber nichts mit dem Kernel, sondern mit der Webanbindung zu tun – die ActiveX-Schnittstelle. Microsoft hat sie mit dem Internet Explorer 3 noch im letzten Jahrtausend eingeführt, um die Browserfunktionalitäten zu erweitern. ActiveX-Module werden von Softwareherstellern bevorzugt verwendet, um Browser-Plug-ins oder Programm-Updates für lokal installierte Programme einzuspielen.

Seit 15 Jahren fehlt für ActiveX ein strengentes Sicherheitskonzept. Stattdessen überlässt es Microsoft den Programmierern, ihr ActiveX-Modul abzusichern. Die Folgen spüren User noch heute: ActiveX führt die Liste der häufigsten Browserlücken an – für die letzten drei Jahre zählt die Vulnerability Database der U.S.-Regierung 338 ActiveX-Bugs. Microsoft selbst geht davon aus, dass „die Hälfte der ActiveX-Steuerelemente, die zur Ausführung auf einer Website vorgesehen sind, keine standardmäßige Sicherheit aufweisen und missbraucht werden können".

ActiveX sollte man daher generell aus dem Wege gehen. Das lässt sich am besten

„Wir dokumentieren nicht alle Security-Lücken in Windows"

Mike Reavey, Direktor des Microsoft-Sicherheitsteams

Ist Windows ein Spion?

Dass große Unternehmen Daten sammeln, daran haben wir uns gewöhnt. Google und Facebook (siehe Artikel auf ► S. 46) etwa wirken mit ihren riesigen Datensammlungen beängstigend. Auch Windows sendet ungefragt Daten an Microsoft. Wir sagen Ihnen, was das Betriebssystem übermittelt, wie Sie das abstellen und was das für Konsequenzen hat.

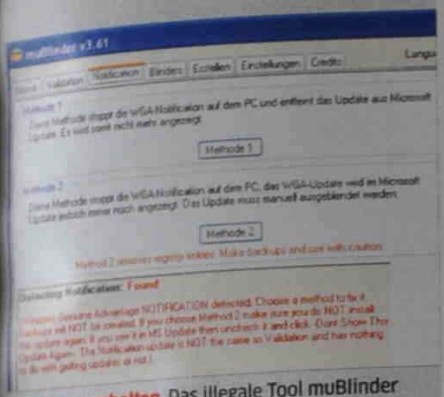
WINDOWS GENUINE ADVANTAGE

Die Echtheitsüberprüfung soll sicherstellen, dass Sie ein korrekt erworbenes Windows nutzen. Dazu checkt sie die Hardware mittels einer BIOS-Prüfsumme, der MAC-Adresse und der Seriennummer der Festplatte. Zusätzlich sammelt sie Informationen über das System wie Product-ID und Activation-Key. Windows Genuine Adavantage (WGA) per Hand zu löschen, ist kompliziert, deshalb gibt es Tools wie muBlinder, die das für Sie erledigen. Da diese einen Kopierschutz aushebeln, ist ihre Nutzung nach deutschem Recht aber nicht legal. Wenn Sie die WGA entfernen, erhalten Sie nur noch die kritischen Sicherheitsupdates.

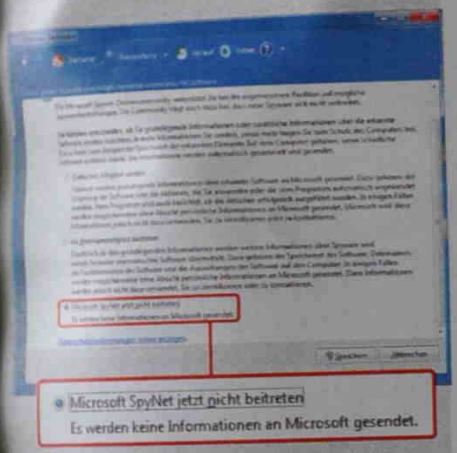
MICROSOFT SPYNET

Über die integrierte Anti-Spyware Defender und den optionalen Virenwächter Security Essentials ist jeder User Teilnehmer des SpyNets. Wird eine der beiden Komponenten alarmiert, sendet sie Informationen über diese Gefahr an Microsoft. Bei den Daten handelt es sich um die IP-Adresse und die Windows- sowie Browserversion. Hinzu kommen Details wie Formular- und Suchdaten, eventuell ein Mini-Speicherabbild oder Informationen, woher die Spyware stammt. Sie können im Defender aus dem SpyNet austreten, und zwar über die Option »Extras | Microsoft SpyNet | SpyNet jetzt nicht beitreten«.
Nutzen Sie die Essentials, dann navigieren Sie in der Registry nach »HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware\SpyNet« und ändern den Key »SpyNetReporting« auf »0«. Unter

Windows 7 müssen Sie sich den Zugriff auf den Key zusätzlich freischalten. Das geht in der Registry mit einem Rechtsklick auf »SpyNet | Berechtigungen«. Deaktivieren Sie die Funktion, so verlieren Sie die Verbindung mit dem Dynamic Signature Service, der beide Microsoft-Programme in Echtzeit mit neuen Signaturen versorgt.

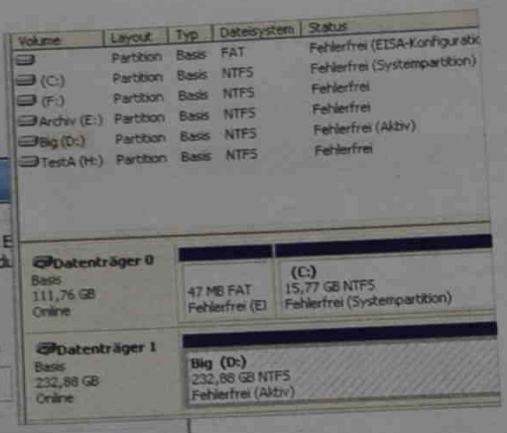


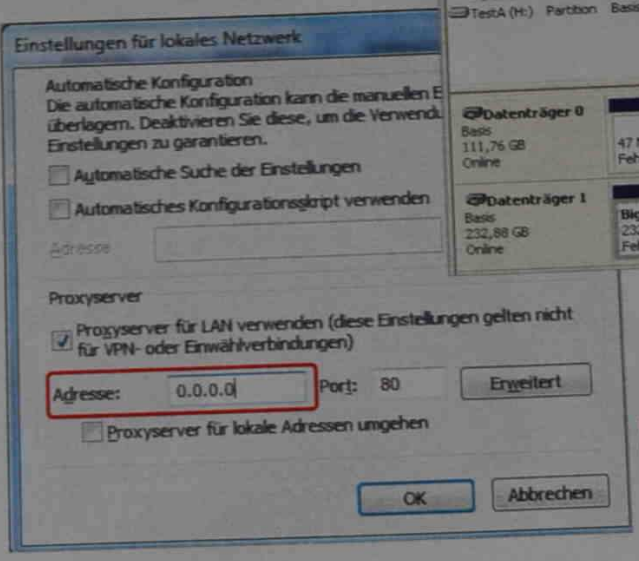
WGA ausschalten Das illegale Tool muBlinder blockiert den Echtheitscheck und ermöglicht das Herunterladen der fehlenden Patches



SpyNet deaktivieren Im Defender können Sie den Bericht an Microsoft über das Verhalten verdächtiger Software abschalten

Zerstörerisch Partitionieren Sie mit XP, so vernichten Sie alle in Windows 7 erstellten Partitionen





IE blocken Sie können den IE per Pseudo-Proxy vom Web trennen. Die Windows-Updates funktionieren dann jedoch nicht mehr

über einen Browser realisieren, der kein ActiveX verwendet und seine Erweiterungen zusätzlich absichert. Momentan haben der Google-Browser Chrome und Firefox 4 für diesen Fall das beste Konzept.

UNZUVERLÄSSIG

Lücken bleiben jahrelang ungepatcht

Jeden ersten Dienstag im Monat erscheinen zuverlässig die neuesten Sicherheitspatches von Microsoft. Doch selbst User, die diese automatisch einspielen lassen, schließen damit längst nicht alle bekannten Windows-Lücken. Die in den Augen des Konzerns unwichtigen Schwachstellen lässt Microsoft offen – manchmal jahrelang.

So vertraut die Windows File Protection (WFP) in XP seit 2002 ohne Überprüfung allen digital signierten Zertifikaten. Die WFP soll eigentlich verhindern, dass Systemdateien verändert werden: Versucht Malware eine solche Datei zu löschen, stellt die WFP sie automatisch wieder her. Im Sommer 2010 meldete nun der Sicherheitsspezialist F-Secure, dass immer mehr Malware zur Manipulation von Systemdateien eine digitale Signatur mitbringt, um genau diese Windows-Hürde zu umgehen – 400.000 signierte Samples zählt F-Secure bis heute. Da der XP-Support abgesehen von Sicherheitspatches ausgelaufen ist, wird sich an dem Zustand auch nichts mehr ändern.

Problematisch wird ein fehlender Patch auch dann, wenn der Browser betroffen ist. Vor etwa zwei Jahren hat der Sicherheitsspezialist Chris Evans auf ein generelles Problem bei der Verarbeitung von JavaScript in allen Browsern hingewiesen, das den Diebstahl von Zugangsdaten ermöglicht, indem es die Same Origin Policy aushebelt. Die Policy besagt, dass Skripte nur auf fremde Inhalte zugreifen dürfen, wenn sie aus derselben Onlinequelle stammen.

Die anderen Browserhersteller haben ihre Produkte diesbezüglich längst abgesichert, doch Microsoft vertritt beim IE8 den Standpunkt, solange die Schwäche nicht in großem Stil ausgenutzt werde, handle es sich um ein geringfügiges Problem. Komisch nur, dass in der Beta des IE9 die Lücke geschlossen ist. Den zugeknöpften Umgang mit Lücken demonstriert auch das Aufspielen stiller Security-Patches, die heimlich undokumentierte Lücken stopfen. Gleichzeitig schmückt sich der Konzern gerne mit Statistiken, die zeigen, dass andere Hersteller mehr Lücken in ihrer Software haben.

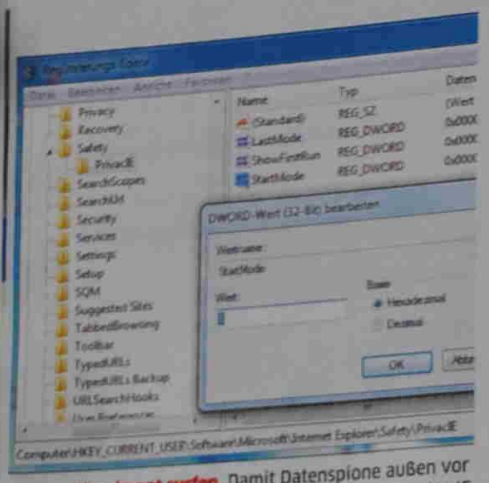
VERLOGEN

Werbekampagne für veralteten IE8

Unter dem Schlagwort „Mit Sicherheit ins Internet" hat Microsoft im März 2010 eine viermonatige Werbekampagne für den Internet Explorer 8 gestartet, um dessen Image aufzupolieren. Was die Sicherheit angeht, so hat sie sich gegenüber dem IE7 in der Tat verbessert. Sonst bietet er keine Features, die die Konkurrenz nicht auch beherrscht, wie etwa den Private Mode, der keine Surfspuren zurücklässt. Im Gegenteil, andere Sicherheitsfeatures wie der Schutz vor Cross-Site-Scripting verursachten immer wieder massive Probleme (siehe Rubrik „Kaputt"). Und noch Anfang November 2010 hatte der Smart Screen Filter einen heftigen Aussetzer. Eigentlich soll er Surfer vor Phishingseiten warnen. Stattdessen blockierte er Webseiten von Banken und anderen Finanzdienstleistern wie etwa Visa.

Das wäre alles nicht so schlimm, wenn man den Browser einfach deinstallieren könnte. Das geht aber nicht, er lässt sich bestenfalls deaktivieren. So nutzt das Betriebssystem die Engine des Browsers weiterhin, wenn es sich mit dem Web verbindet, um beispielsweise Updates einzuspielen. Allerdings können Sie das verhindern: Schalten Sie im Internet Explorer in den »Extras | Internetoptionen« unter »Verbindungen | LAN-Einstellungen« auf »Proxy Server für LAN-Einstellungen verwenden« und geben Sie unter »Adresse« eine IP an wie »0.0.0.0«, die ins Datennirwana umleitet.

Achtung: Das wird problematisch, wenn andere Software, die Sie nicht blockieren wollen, über die IE-Einstellungen ins Netz will. Ob man den Browser wirklich abklemmen sollte, muss also jeder für sich entscheiden. →



Unerkannt surfen Damit Datenspione außen vor bleiben, aktivieren Sie den InPrivate-Filter des IE über einen Eintrag in der Registry

KAPUTT

Securityfunktionen taugen nichts

Die Werbekampagne für IE8 hat noch einen anderen Schönheitsfehler: Neben dem Smart Screen Filter sollte ein Schutz gegen Cross-Site-Scripting (XSS) den Surfer vor Webattacken bewahren. XSS erlaubt, dass ein Angreifer auf vertrauenswürdigen Webseiten Schadcode ausführt, meist über einen manipulierten Link. Immer noch sind viele Sites – auch von Banken – offen für XSS, daher ist ein Filter durchaus sinnvoll.

Als die Kampagne anlief, musste Microsoft den Filter zum dritten Mal per Patch reparieren. Er ließ sich so manipulieren, dass er sichere Webseiten wie die Google-Suche wieder verwundbar machte. Im Gegensatz zu anderen XSS-Blockern wie dem Firefox-Add-on NoScript (auf Heft-DVD) greift der Microsoft-Filter nicht ein, wenn der XSS-Code vom Browser zum Server geschickt wird. Er wird erst aktiv, wenn der XSS-Code serverseitig bearbeitet wieder an den Browser zurückgeht. Nur durch das späte Eingreifen kann eine Sicherheitslücke im Filter selbst den XSS-Schutz der Webseite aufheben.

Für diesen Aussetzer hat Microsoft auf der Sicherheitsmesse Black Hat 2010 die Negativauszeichnung „Most Epic FAIL" erhalten. Die hätte auch sein Virenscanner verdient, der zur selben Zeit wie Vista unter dem Namen OneCare auf den Markt kam: Als einer der wenigen versagte er beim renommierten Virus-Bulletin-Test, als er über 18 Prozent der Schädlinge nicht erkannte.

Mittlerweile nennt sich das Produkt Security Essentials und liegt, was die signaturbasierte Erkennung angeht, gleichauf mit der Konkurrenz. Allerdings fehlt den Essentials immer noch das verhaltensbasierte Aufspüren bisher unbekannter Viren.

Die geheimen Stärken von Windows

Microsoft hat nicht nur gesündigt. Gerade die neuen Funktionen von Vista und Windows 7 widersprechen dem landläufigen Vorurteil vom langsamen und unsicheren Betriebssystem.

SPEICHERSCHUTZ: Seit Vista gilt Windows als System, das im Prinzip schwerer zu knacken ist als Linux oder Mac OS X. Der Grund sind ASLR (Address Space Layout Randomization) und DEP (Data Execution Prevention), zwei Techniken, welche die Daten im Arbeitsspeicher für Hacker schwerer zugänglich machen.

SSD-FUNKTIONEN: Windows 7 ist das erste Betriebsystem, das die neuen, schnellen Flashfestplatten korrekt identifiziert und die Systemfunktionen entsprechend anpasst. Zusätzlich kann Windows 7 mittels TRIM-Befehl die Lebensdauer von SSDs verlängern.

GPU-BESCHLEUNIGUNG: Mit Windows 7 sind die Hardware-Anforderungen für die Wiedergabe von High-Definition-Material stark gesunken. Der Grund: Die im System integrierten Abspielfilter nutzen die Hardware-Beschleunigung des Grafikchips zum Dekodieren der Filme, wenn es dessen Treiber zulässt.

SCHIZOPHREN

Entwickler torpedieren Features

Bei Microsoft konkurrieren viele Teams, die verschiedene Produkte und Services vertreten. Das bekommen auch Windows-User zu spüren. So plante das IE-Entwicklerteam, die Version 8 mit aktiviertem InPrivate-Filter zu starten. Zudem sollte der Browser die Funktion InPrivate Subscriptions erhalten, die anhand einer Blacklist Tracking-Webseiten sperrt, die den User ausspionieren. Da Microsoft auch als Werbevermarkter aktiv ist, wurde das Feature gestrichen.

Wollen Sie den InPrivate-Filter sinnvoll nutzen, schalten Sie ihn mittels eines Eintrags in der Registry permanent ein. Navigieren Sie hier zu »HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Safety\PrivacIE« und erzeugen Sie den DWORD-Schlüssel »StartMode« mit dem Wert »1«. Unter Umständen müssen Sie die Schlüssel ab »Safety« vorher selbst anlegen. Auch den Private Mode, der alle Surfspuren löscht, können Sie automatisch zum Browserstart aktivieren. Dazu kopieren Sie das Desktop-Icon des IE und ergänzen in den »Eigenschaften« der Kopie unter »Verknüpfung | Ziel« am Ende das Attribut »-private«.

Nicht immer haben interne Streitigkeiten direkt Auswirkungen auf Windows. Momentan steht die Weiterentwicklung von Microsofts Flash-Alternative Silverlight für die Windows-Plattform infrage. Leitende Microsoft-Manager haben den Fokus von Silverlight auf HTML5 gelegt. Für Scott Barnes, einen ehemaligen Produktmanager der Windows Presentation Foundation (WPF), hätte das weitreichende Konsequenzen: Von der Codebasis her ist die WPF der Überbau für Silverlight, dient aber gleichzeitig als Standardframework für die Entwicklung von Programmoberflächen. Sollte Silverlight nur noch für Spezialaufgaben oder Windows Phone 7 eingesetzt werden, bedeutet das auch für die WPF das Aus. Barnes befürchtet gar, dass HTML5 künftig auch die WPF als Programmoberfläche für Windows-Software ersetzen könnte – und das wirft neue Sicherheitsprobleme auf.

VERALTET

Das Zubehör besteht aus Crapware

Seit seinen Anfängen hat Windows eine Reihe von Tools im Gepäck wie Notepad oder Paint. Dieses „Zubehör" kann sich selten mit externer Software messen. In Windows 7 wurde die Zusatzausstattung im Multimedia-Bereich aufgewertet. XP-User müssen sich mit zweitklassigen Funktionen herumschlagen.

Mit Paint enthält Windows eine rudimentäre Bildbearbeitung, die von Masken, Ebenen und Histogrammen keine Ahnung hat. Das ist besonders enttäuschend, da Microsoft zusammen mit der Washington State University das leistungsstarke Paint.NET (auf Heft-DVD) entwickelt hat. Über das Paint.NET PSD Plug-in (auf DVD) können Sie sogar Photoshop-Dateien bearbeiten. Der einfache Texteditor Notepad kann außer dem Zeilenumbruch gar nichts. Die Open-Source-Variante Notepad++ (auf DVD) bietet dagegen eine Rechtschreibprüfung und lässt sich durch Plug-ins erweitern.

Windows bringt zwar eine interne Packfunktion mit, doch sie beherrscht nur das ZIP-Format. Im Web sind mittlerweile RAR und 7z die Standardformate, die das Tool 7-Zip (auf DVD) auch problemlos entpackt. Die Brennfunktion von XP beschränkt sich auf das Beschreiben von CDs. Nutzen Sie stattdessen die Vollversion Burning Studio Elements von der Heft-DVD, sie brennt auch DVDs und Blu-ray-Scheiben. Für ein schnelleres Dateimanagement sollten Sie den Windows-Explorer durch Q-Dir ersetzen oder mit QTTabBar aufrüsten (beides auf DVD).

Als User muss man eben immer noch selbst Hand anlegen, um das System zu optimieren. Microsoft allein wird das wohl auch in Zukunft nicht schaffen.

MARKUS.MANDAU@CHIP.DE