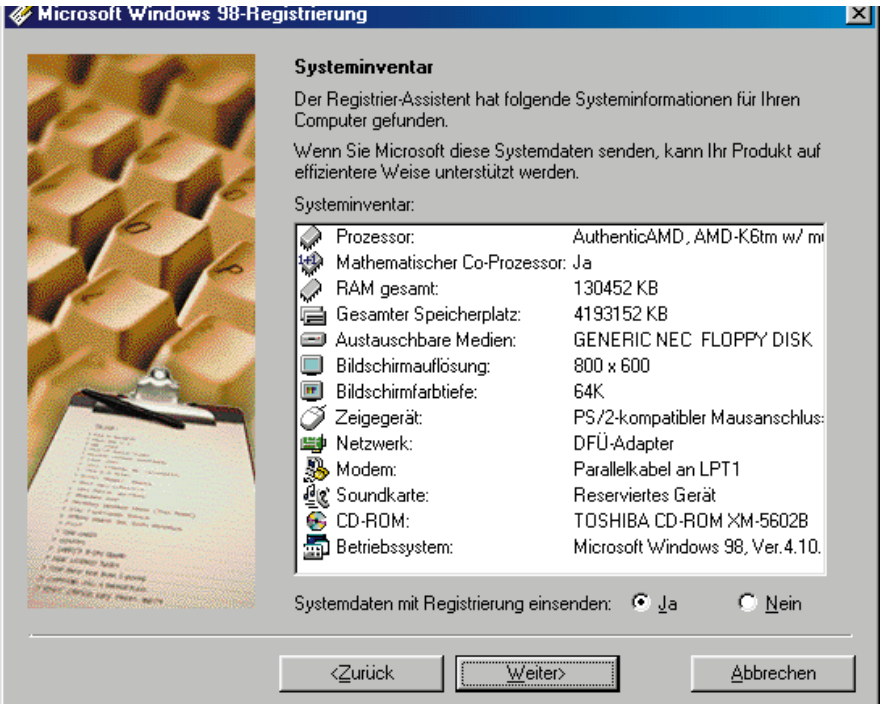
Was Microsoft alles über Sie weiß

Big Brother Microsoft?

Wenn Sie sich bei Microsoft online registrieren lassen, bekommen Sie kostenlose Treiber-Updates und Online-Support. Eine feine Sache – an sich.
Doch was ist dran an den Gerüchten, daß Microsoft dabei Ihr komplettes System ausspioniert?



Das Systeminventar: Diese hier angezeigten Hardware-Informationen findet der Registrierungs-Wizard in den einschlägigen Registry-Schlüsseln

Microsoft spioniert PCs aus – solche Vorwürfe können Sie im Internet unter ***http://www.dejanews.com/*** lesen. Grund für die Aufregung sind angebliche Schnüffeleien auf der Festplatte während der sogenannten Online-Registrierung. Zu der Registrierung werden Sie bei der Installation von Windows oder anderen MS-Produkten aufgerufen; unumgänglich ist sie für Treiber-Updates oder die Installation von neuen Treibern („Treiber aktualisieren" im Geräte-Manager) über das Internet.

Wir wollten wissen: Was passiert wirklich? Auf den ersten Blick sendet die Registrierungsroutine nur einige Kundendaten, außerdem ein paar Infos über den PC, die sich laut Dialogliste („Systeminventar") auf Hardware-Informationen wie CPU oder RAM-Ausstattung beschränken.

Man traut aber offenbar Microsoft alles Schlechte dieser Welt zu. Denn obwohl das Ganze ebenso harmlos wie seriös wirkt, brodelt die Gerüchteküche: Schickt der Update-Dienst in Wahrheit andere Informationen, etwa über die Software-Ausstattung und etwaige Raubkopien, an den Microsoft-Server?

PC WELT INFO

MS-Datenspionage?

Bei der Online-Registrierung verschicken Sie Daten an den Software-Hersteller. Gerüchte wollen nicht verstummen, daß Microsoft bei dieser Aktion gleich die gesamte Software-Ausstattung erfaßt. Die PC-WELT ist dem Vorwurf am Beispiel der Windows-98-Registrierung nachgegangen.
Resultat: Entwarnung ist angesagt.

VERSCHLÜSSELTE DATEN

Wir testen mit Comspy

Um herauszufinden, welche Informationen übers Internet wandern, wäre es am einfachsten, die bei der Registrierung gesendeten Daten direkt zu lesen. Wir haben das versucht – unter anderem mit dem Freeware-Utility Comspy (***http://www.spywindows.com/page1/software.htm***). Die Online-Registrierung übermittelt die Daten jedoch nicht im Klartext, sondern in verschlüsselter Form – das ist aus Gründen des Datenschutzes notwendig und Microsoft nicht vorzuwerfen. Auf diesem Weg war daher bloß zu erfahren, daß das Registrierungsprogramm nur wenige Daten verschickt. Daß also etwa, wie die Flüsterpropaganda besagt, ein kompletter Registry-Export stattfindet oder die HWINFO.DAT an Microsoft geht, die Infos über die vollständige Software-Konfiguration enthält, ist schon aufgrund der Datenmenge auszuschließen.

Da es nicht gelang, auf diese Weise die gesendeten Infos zu ermitteln, schlugen wir einen indirekten Weg ein. Die Fragestellung war: Was kann das Registrierungsprogramm (Regwiz) über die Software-Ausstattung wissen? Um herauszufinden, wofür sich Regwiz interessiert, haben wir uns bei Microsoft einige Tage rund um die Uhr registrieren lassen. (Vielleicht wird Microsoft unseren „Christian Löwenzahn, Semmelbach 3, 20345 Hamburg", zum „Kunden des Jahres 1998" küren ...)

Beim Registrieren haben wir drei Systemkomponenten überwacht und sind

den folgenden Fragen nachgegangen:
• Sucht Regwiz im Dateisystem nach Dateinamen bekannter Software?
• Sucht Regwiz in der Registry nach installierter Software?
• Und ganz wichtig: Öffnet Regwiz Dateien, die Software-spezifische Informationen enthalten?

REGWIZ-KONTROLLE (I)

Schnüffler auf der Festplatte?

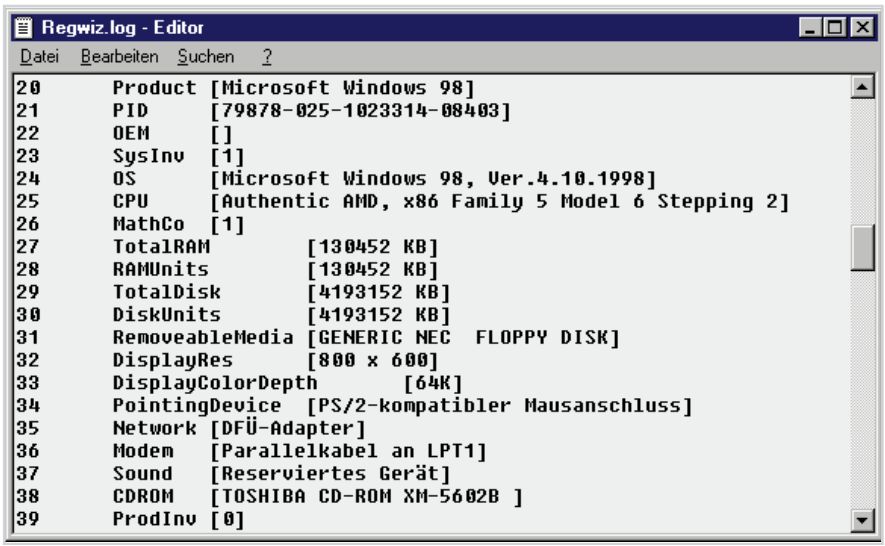
Wenn Sie sich bei Microsoft online registrieren lassen, stellen Sie subjektiv keine intensive Suche auf der Festplatte fest: Der Vorgang ist – abgesehen von den benutzerspezifischen Eingaben – schnell erledigt, und die LED für die Harddisk-Aktivität blinkt nur sporadisch. Wir fanden diesen Eindruck bestätigt, nachdem wir mit der Freeware Vxdmon von Cogswell/Russinovich (***http://www.sysinternals.com/vxdmon.htm***) insbesondere die Aktivität des Windows-eigenen IFS-Managers (Installable File System) überwacht hatten. Während der IFS-Manager bei „Suchen nach“ oder während eines DIR-Befehls Tausende von Zugriffen meldet, finden hier nur wenige Zugriffe auf das Dateisystem statt. REGWIZ.EXE erstellt unter anderem eine neue Datei (→ nächster Punkt). Suchaktionen im Dateisystem finden definitiv nicht statt.

REGWIZ-KONTROLLE (II)

Schnüffler in der Registry?

Die Registry wäre mit Sicherheit ein ergiebiges Ziel für eine Schnüffelaktion nach illegaler Software: Sie enthält die wesentlichen Angaben und befindet sich permanent im Speicher, so daß ein schneller und vom Normalanwender unbemerkter Zugriff möglich wäre. Aber es gibt Kontroll-Utilities, die solche Leseaktionen protokollieren. Wir benutzten REGMON.EXE (ebenfalls von den oben genannten Autoren, ***http://www.sysinternals.com/regmon.htm***). Damit ist nachzuweisen, daß Regwiz in der Tat Registry-Informationen ausliest. Allerdings handelt es sich dabei fast ausschließlich um Hardware-Angaben, daneben um die „SubVersion Number“ und die „ProductID“.

Was Regwiz sucht und findet, dürfte auch den mißtrauischsten Anwender nicht beunruhigen. Auch bleibt alles



REGWIZ.LOG: Die Datei enthält lediglich die Benutzerangaben sowie einige Infos zur Hardware, zur Windows-Version und zu deren Produkt-ID

transparent: Eben diese Infos listet der nachfolgende Dialog „Systeminventar“ auf – und Sie haben die Möglichkeit, das Systeminventar nicht zu verschicken – indem Sie „Nein“ aktivieren. Daß ein „Nein“ wirklich ein Veto bedeutet, belegt unser dritter Kontrollschritt.

REGWIZ-KONTROLLE (III)

Zugriff auf Systemdateien?

Mit dem Freeware-Utility FILEMON.EXE (***http://www.sysinternals.com/filemon.htm***) kontrollierten wir die Dateizugriffe, die während der Online-Registrierung erfolgten. Es bestätigte sich, daß keine Suche auf der Festplatte stattfindet. Allerdings bleiben einige Zugriffe auf Dateien suspekt: Regwiz öffnet die WIN.INI und später die OEMINFO.INI. Die WIN.INI enthält Software-spezifische Informationen. Daß Microsoft diese bei der Registrierung verschickt, ist jedoch aufgrund der späteren Aktionen unwahrscheinlich. Wer dennoch auf Nummer Sicher gehen will, kann diese beiden Dateien vor der Registrierung einfach umbenennen.

Regwiz greift erst auf einige Internet-spezifische DLLs zu, um die Verbindung herzustellen, und erstellt dann die Datei REGINFO.TXT, die die Benutzerdaten sowie die ermittelten Hardware-Informationen enthält.

Welche Datei verschickt Regwiz übers Netz? Wir tippen auf die temporäre Datei REGWIZ.LOG im Temp-Verzeichnis. Sie unterscheidet sich inhaltlich kaum von der vorher angelegten TXT-Datei. Lediglich der Rechnername wird zusätzlich aufgeführt, falls es sich um einen Netz-PC handelt. Hardware-Infos sind nicht enthalten, wenn der Anwender im Dialog „Systeminventar“ die Option „Nein“ gewählt hat.

DIE FAKTEN

Big Brother Microsoft?

Wegen der Datenverschlüsselung bleibt offen, welche Informationen exakt an den Microsoft-Server gehen. Die Menge der gesendeten Daten ist jedoch gering; sie reicht nicht aus, um etwa den Schlüssel „Software“ aus der Registry zu übermitteln. Auch konnten wir feststellen, auf welche Quellen der Registrierungs-Wizard zugreift, bevor er Daten verschickt. Diese Quellen enthalten nach unserer Kenntnis keine relevanten Informationen über die Software-Ausstattung. Die Inspektion der WIN.INI ist verdächtig, dient aber wohl nur der Suche nach älterer Internet-Software.

Die von Regwiz neu angelegte REGWIZ.LOG ist – das legen Größe und Inhalt nahe – vermutlich das Sendeprotokoll. Sie enthält die eingegebenen Benutzerdaten und die Hardware-Infos, die der Dialog „Systeminventar“ zeigt.

Man muß kein Microsoft-Fan sein, um den Vorwurf der Datenspionage hier ad acta zu legen. Daß Sie und wir künftig trotzdem wachsam bleiben müssen, versteht sich von selbst.

H. APFELBÖCK / TH. EGGELING