nen. Um sie für eine Datei zu aktivieren, öffnen Sie in deren Kontextmenü *Eigenschaften* und klicken im Reiter *Allgemein* auf die Schaltfläche *Erweitet*. Aktivieren Sie hier die Option *Inhalt verschlüsseln, um Daten zu schützen* und bestätigen Sie mit *OK*.

Arpoon Checksum 1.6

Prüfsummen checken

Mit einer Prüfsumme lässt sich die Integrität heruntergeladener Programme feststellen. Arpoon Checksum 1.6 (**www.arpoon.de/checksum.html**, kostenlos) zeigt Ihnen die Prüfsumme einer Datei an, die Sie dann mit der des Herstellers vergleichen. Starten Sie das Tool per Doppelklick. Wählen Sie dann über *File*, *Options* den gewünschten Algorithmus aus. Drücken Sie *[Strg]+[O]* und wählen Sie eine Datei aus, damit das Tool deren Prüfsumme anzeigt.

Open Office

Private Daten löschen

In den Eigenschaften eines Dokuments speichert Open Office auch private Daten: etwa Ihren Benutzernamen, wann es von wem zuletzt verändert und wann es zuletzt gedruckt wurde. Bei der Weitergabe von Dokumenten sind diese Infos aber nicht immer erwünscht. Über den Menüpunkt *Datei*, *Eigenschaften* sehen Sie die gespeicherten Informationen ein. Um sie zu entfernen, deaktivieren Sie hier die Option *Benutzerdaten verwenden*, klicken auf *Löschen* und bestätigen mit *OK*.

Windows Vista

Papierkorb deaktivieren

Statt Dateien beim Löschen zunächst in den Papierkorb zu verschieben, können Sie diese auch direkt löschen. So verrät der nun überflüssige Papierkorb nicht mehr, welche Dateien Sie entfernt haben. Öffnen Sie dafür per Rechtsklick auf den Papierkorb den Kontextmenüpunkt *Eigenschaften* und aktivieren Sie *Dateien sofort löschen (nicht in Papierkorb verschieben)*. Den Papierkorb entfernen Sie, indem Sie mit der rechten Maustaste auf den Desktop klicken, *Anpassen* und dann *Desktopsymbole ändern* wählen. Deaktivieren Sie hier *Papierkorb*.

Freier Virenscanner

Clam-AV schliesst Leck

Der Antiviren-Scanner Clam-AV ist anfällig für manipulierte Dateien im HTML- und Rich-Text-Format (RTF). Sie können ihn abstürzen lassen. In Version 0.91.2 ist der Fehler behoben. Den Open-Source-Scanner Clam-AV hat Sourcefire kürzlich übernommen.
www.clamav.net

Yahoo und Microsoft betroffen

Lücken in Messengern

Wenn Anwender des MSN-Messengers der Versionen 6 und 7 die Einladung zu einem Video-Chat annehmen, ist ein Angreifer in der Lage, einen Pufferüberlauf herbeizuführen. Die übertragenen Daten werden dann ungeprüft ausgeführt. Ein ähnlicher Fehler wurde kürzlich beim Yahoo-Messenger behoben.
http://secunia.com/advisories/26570, http://secunia.com/advisories/26501

Software versteckt Rootkit-Funktion

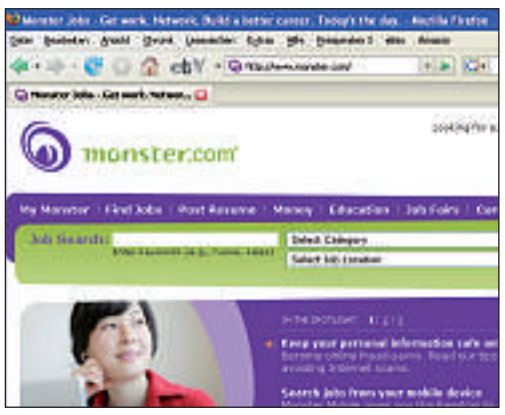
Korrupter USB-Stick

Sony BMG hat USB-Sticks in den Handel gebracht, deren Software sich ähnlich wie ein Rootkit auf dem Rechner einschleicht. Die Sticks der Marke Microvault enthalten dem Sicherheitsunternehmen F-Secure zufolge einen Fingerabdrucksensor, dessen Software sich in einem versteckten Verzeichnis unter C:\WINDOWS einnistet. Angreifer verbergen dort möglicherweise Schadcode vor dem Anwender und vor Sicherheitsprogrammen. Sony hat den Verkauf der Sticks inzwischen gestoppt und plant einen Software-Patch.
www.f-secure.com/weblog

Monster.com gehackt

Jobsucher ausspioniert

Der Trojaner Infostealer.Monstres hat die persönlichen Daten Arbeitssuchender ausspioniert – von 1.6 Millionen Datensätzen insbesondere aus den USA ist die Rede. Der Trojaner verbreitet sich über E-Mail-Anhänge und Websites, soll aber auch in Werbung auf Monster.com gewesen sein. Offenbar versuchen die Kriminellen, mit den gestohlenen Daten Geldwäscher zu rekrutieren.
www.symantec.de



Gehackt: Nutzerdaten bei Monster.com

Zugriff auf Domains

Phisher gegen Registrare

Phisher haben eine neue Gruppe ins Visier genommen: Die Kunden von Domain-Registraren. Eines der ersten Opfer ist US-Registrar Godaddy.com. Per E-Mail werden dessen Kunden aufgefordert, persönliche Angaben in einem Webformular einzutragen. Der Link zum Formular führt zu einem Go-Daddy-Klon. Die Phisher verschaffen sich auf diese Weise die Kontrolle über die Domains und nutzen diese anschliessend für ihre Zwecke.
www.domain-recht.de

Video-Virus der Sturm-Wurm-Bande

Trojaner tarnt sich als Youtube-Video

Websense Security Labs warnen vor einem Trojaner, der sich als Youtube-Clip tarnt. E-Mails und Blogs fordern dazu auf, einen Link zu einem angeblichen Youtube-Video zu öffnen. Um den Nutzer zum Klicken zu verlocken, suggerieren die Betreff-Zeilen, es handle sich um ein Video, das für den Anwender peinlich ist. Der Link führt statt zu Youtube zu einer Seite mit Malware.
www.websense.com/securitylabs/alert/alert.php?AlertID=799

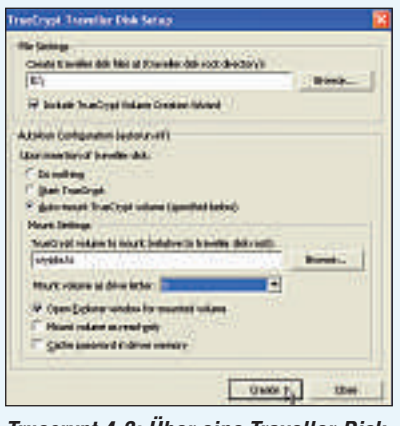
SICHERHEITS-TIPP DES MONATS: TRAVELLER-MODE VON TRUECRYPT

Truecrypt verschlüsselt auch die Daten auf Ihrem USB-Stick. Im Traveller-Mode greifen Sie auf fremden PCs auf Ihre Daten zu.

Wer Truecrypt 4.3 (**www.truecrypt.org**, kostenlos) auf fremden Rechnern einsetzen möchte, dort aber keine Software installieren will, nutzt den Traveller Mode. Dabei bringen Sie Truecrypt auf dem USB-Stick mit. Allerdings benötigen Sie dazu Administratorrechte. Sie starten Truecrypt per Mausklick auf die Datei *truecrypt.exe* auf dem USB-Stick.

Richten Sie auf dem USB-Stick noch eine Traveller-Disk ein, dann geht das Einbinden der darauf abgelegten Volumes fast von allein. Die Traveller-Disk enthält die ausführbaren Truecrypt-Dateien sowie die Datei *autorun.inf*. Diese sorgt dafür, dass Truecrypt beim Anstecken des Sticks automatisch startet und ein bestimmtes Truecrypt-Volume mountet. Diese Funktion setzt eine aktivierte Autorun-Funktion sowie Windows XP mit SP2 oder Vista voraus.

Um eine Traveller-Disk einzurichten, starten Sie Truecrypt und wählen *Tools, Traveller Disk Setup*. Navigieren Sie zunächst oben über *Browse…* zu Ihrem USB-Stick. Möchten Sie ein bestimmtes Volume automatisch einbinden, aktivieren Sie *Auto-mount TrueCrypt volume (specified below)* und wechseln über *Browse…* zum gewünschten Volume. Im Dropdown-Menü suchen Sie dann noch einen Laufwerkbuchstaben aus. Belassen Sie den Haken bei *Open Explorer window for mounted volume*, dann öffnet Truecrypt auch den entsprechenden Ordner automatisch. Mit *Create* legen Sie die Disk an.



Truecrypt 4.3: Über eine Traveller-Disk bindet das Tool ein Volume ein.