

Unachtsamkeit wird bestraft

Die zehn besten Tipps, wie Sie Ihre privaten Daten am Computer schützen können

VON REBEKKA RÜLCKER

1 Keine öffentlichen Rechner

Arbeiten Sie mit privaten Daten und vertraulichen Informationen nur am eigenen Rechner. Auf fremden und öffentlichen Computern besteht die Gefahr, dass der Rechner nicht ausreichend gegen Schadsoftware und Angriffe aus dem Internet geschützt ist oder dass nachfolgende Benutzer mit krimineller Energie und technischem Geschick vertrauliche Daten herausfinden.

2 Sicherheitseinstellungen

Installieren Sie ein Virenschutzprogramm und ein Anti-Spyware-Programm. Setzen Sie eine Personal-Firewall ein. Bei richtiger Konfiguration schützt sie vor Angriffen aus dem Internet und verhindert bei einer Infektion des Computers mit einem Schädling, dass ausgespionierte Daten an einen Angreifer gesendet werden. Bietet der Betreiber Ihres E-Mail-Fachs einen Viren-Scanner und einen Spam-Filter, nutzen Sie diese zusätzlich.

3 Halten Sie Ihr System aktuell

Software-Anbieter beheben regelmäßig Sicherheitslücken, indem sie neue Versionen ihrer Produkte anbieten. Bei vielen, etwa beim Betriebssystem Win-

dows, werden diese auf Wunsch automatisch aus dem Internet heruntergeladen und aktualisiert. Der Viren-Scanner sollte seine Informationen mindestens täglich auf den neuesten Stand bringen.

4 Daten geheim halten

Gehen Sie sorgfältig mit Kennwörtern, Benutzernamen und Zugangscodes (Tan, Pin) um. Speichern Sie diese Daten niemals elektronisch, wählen Sie keine naheliegenden Passwörter (wie Geburtsdatum oder eigener Name) und wechseln Sie diese regelmäßig. Wichtig: Banken fordern niemals per Mail auf, vertrauliche Daten bekanntzugeben.

5 Der richtige Browser

Als Faustregel gilt, lieber den Firefox-Browser als den Internet-Explorer verwenden, weil Letzterer wegen seiner großen Verbreitung immer noch Hauptziel von Angriffen ist. Verwenden Sie moderne Browser, viele neuere Ausgaben vergleichen aufgerufene Internetseiten mit Datenbanken von unseriösen Seiten und warnen vor Gefahr.

6 Selber tippen

Verwenden Sie nie Links, die Ihnen per Mail zugesandt wurden – Sie wissen nicht, ob

die Links präpariert wurden. Geben Sie beispielsweise die Startseite Ihrer Bank per Hand ein oder verwenden Sie gespeicherte Favoriten. Nutzen Sie das Log-in-Portal. Deaktivieren Sie im Browser alle Funktionen, die automatisch Usernamen, Passwort oder E-Mail-Adresse ergänzen („Auto-Fill“). Auf diese Daten kann per Schadmail leicht zugegriffen werden.

7 Vorsicht bei Downloads und E-Mail-Anhängen

Schadprogramme werden oft über Dateianhänge verbreitet. Auch hinter Downloads kann sich ein Virus verstecken. Wird Ihnen eine Software zum Download angeboten, folgen Sie nicht dem automatischen Link, sondern suchen Sie die Software über eine Suchmaschine.

8 Nie als Administrator arbeiten

Arbeiten Sie nur im Notfall als Administrator an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines Rechners unterschiedliche Benutzerkonten ein. Vergeben Sie für diese nur die Berechtigungen, die der jeweilige An-

wender für seine Arbeit wirklich braucht. So werden auch private Dateien vor dem Zugriff anderer geschützt.

9 Verschlüsseln

Achten Sie beim Online-Banking darauf, dass eine verschlüsselte Verbindung mit der Website der Bank aufgebaut wird. Bei den meisten Banken ist das eine „SSL-Verschlüsselung“, die immer am „https“ in der Adresszeile erkannt werden kann. Der Browser überprüft automatisch das Zertifikat dieser Seiten und gibt eine Warnmeldung, wenn sich der Anbieter nicht mit einem gültigen Zertifikat als Besitzer der Website ausweisen kann. Achten Sie auch beim Verwenden von Übertragungstechnologien wie „Voice over IP“ (VoIP) oder Wireless-Lan darauf, dass die Kommunikation verschlüsselt



ist, damit Dritte nicht mitlesen beziehungsweise zuhören können.

10 Für den Notfall

Damit wichtige Daten nicht verloren gehen, wenn es zu einer Infektion des Computers kommt, sollten Sie regelmäßig Sicherheitskopien Ihrer Dateien auf CD-ROM/DVD oder einer externen Festplatte erstellen. Überwachen Sie am besten täglich die eigenen Kontobewegungen, um bei eventuellen Missbrauchsfällen schnell die Bank informieren zu können. Drucken Sie getätigte Transaktionen zur lückenlosen Dokumentation aus. Melden Sie Verdächtiges dem jeweiligen Webmaster und bei (vermutetem) kriminellen Hintergrund der Polizei. Sichern Sie betrügerische E-Mails als Beweismaterial.