Bundeskriminalamt

BITKOM

Empfehlungen
für Sicherheit im Internet

6. September 2010

So schützen Sie sich vor Gefahren

1. PC-Schutz
Entscheidend ist eine gute Sicherheitsausstattung Ihres Computers. Vor der ersten Internet-Sitzung müssen ein Anti-Viren-Programm und eine Firewall installiert werden, um den PC vor schädlichen Dateien zu schützen. Für diese Schutzprogramme, das Betriebssystem und den Internet-Browser werden regelmäßig Aktualisierungen angeboten, die auch automatisiert abgerufen werden können. Updates sind umgehend zu installieren. Das gilt auch für auf dem PC installierte Anwendungsprogramme. Da Schadsoftware zunehmend über Datenträger wie CDs oder USB-Sticks verbreitet wird, sollten diese vor der Nutzung auf Viren geprüft werden.

2. E-Mails und Chat
Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen. Dubiose Mails von Unbekannten möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail-Anhängen. Verdächtige Dateien auf keinen Fall öffnen! Vorsicht auch vor angeblichen E-Mails von Kreditinstituten: Banken bitten Kunden nie per Mail, vertrauliche Daten im Netz einzugeben. Solche E-Mails sind immer gefälscht. Auch in Communitys empfangene E-Mail-Anhänge sollten mit einem Schutzprogramm überprüft werden. Riskant können auch Chat-Nachrichten von Unbekannten sein: Kriminelle versenden oft Links zu Webseiten mit Viren.

3. Software
Nutzer sollten darauf achten, welche Software oder Zusatzprogramme („Plug-Ins“) sie installieren. Eine Gefahr sind Schadprogramme, die in Gratis-Downloads oder Raubkopien von dubiosen Anbietern versteckt sind. Gesundes Misstrauen hilft: Wenn Zweifel an der Seriosität bestehen, besser auf Download und Installation einer Software verzichten.

4. Tauschbörsen
Wer im Internet mit Unbekannten Dateien tauscht, riskiert eine Infektion seines PCs mit Schadprogrammen. Zudem ist der Tausch von illegalen Musik-, Film- oder Software-Kopien strafbar und kann zu Schadenersatzansprüchen der Rechteinhaber führen.

5. Online-Shopping
Zeichen für die Seriosität eines Online-Shops sind ein Impressum mit Nennung und Anschrift des Geschäftsführers sowie klare Geschäftsbedingungen (AGB). Kunden sollten auch die Datenschutzerklärung lesen. Manche Shops werden von unabhängigen Experten geprüft und

erhalten ein Zertifikat oder Siegel. Auch der Kunde kann Kontrolle ausüben: Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Händler beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein.

6. Bezahlung im Web
Zur Bezahlung müssen Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an den Buchstaben „https“ in der Adresse der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Sichere Webseiten sind auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahl-Dienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist verbreitet, aber riskanter.

7. Online-Banking
Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder über eigene Lesezeichen (Favoriten) aufrufen. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Verbindung zum Bankcomputer muss wie bei Bezahlvorgängen verschlüsselt sein. Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen solchen Code aus einer Liste frei wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN aus der Liste eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren: Die TAN wird dem Kunden aufs Handy geschickt und ist nur kurzzeitig gültig. Weitere Schutzverfahren sind eTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TAN-Generator oder ein Kartenlesegerät nutzt. PC-Nutzer sollten ihre Bank fragen und das modernste verfügbare Verfahren wählen. Vorsicht, falls mehrere Transaktionsnummern auf einmal abgefragt werden: Dann ist Phishing im Spiel – gleich die Bank informieren.

8. Private Infos
Die meisten Menschen würden im Alltag kaum Unbekannten ihr Privatleben offenbaren. Auch im Web haben es die Nutzer in der Hand, den Zugang zu privaten Infos zu beschränken. Nur gute Bekannte sollten in entsprechenden Foren und Communitys Zugriff auf Fotos oder Kontaktdaten erhalten. Je weniger von der eigenen Privatsphäre frei zugänglich ist, desto weniger Angriffsfläche wird potenziellen Betrügern und anderen unbefugten Nutzern geboten.

9. Passwörter
Bei vielen Online-Services müssen sich die Nutzer registrieren. Meist werden Benutzername und Passwort festgelegt. Soweit möglich, sollten Kunden nicht das gleiche Passwort für mehrere Dienste verwenden – etwa E-Mail-Konto, Online-Shops und Communitys. Je länger ein Passwort, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Wer sich die zahlreichen Codes schwer merken kann, dem helfen so genannte Passwort-Safes. Das sind PC-Programme, mit denen sich Geheimzahlen sicher speichern lassen. Der Anwender braucht sich dann nur noch ein Haupt-Passwort zu merken.

10. Angebote als Waren- oder Finanzagenten
Angebote im Internet oder per E-Mail, als Waren- oder Geldvermittler zu arbeiten, sind konsequent abzulehnen. Der Vermittler dient den Tätern zur Verschleierung ihrer Identität. Web-Nutzer, die sich auf dubiose Angebote einlassen und Waren oder Gelder weiterleiten, können sich strafbar machen und müssen mit Schadenersatzansprüchen rechnen.