Tipps für Bürger

"Goldene Regeln" für mehr Sicherheit

Das Surfen im Internet soll in erster Linie informieren und Spaß machen. Aber es birgt auch durchaus einige Risiken, gegen die man bereits durch Aufmerksamkeit und verschiedene zusätzliche Maßnahmen gut vorbeugen kann, um den eigenen PC beim Surfen im Internet sicherer zu machen.
Einen Ausschnitt daraus wollen wir Ihnen im Folgenden kurz vorstellen. Auf den ersten Blick klingt manches sicher simpel und einleuchtend, wird aber dennoch oft genug mißachtet. Die Angaben erheben natürlich keinen Anspruch auf Vollständigkeit.

1. Surfen Sie nach Möglichkeit nicht mit einem PC im Internet auf dem Sie sicherheitskritische oder personenbezogene Daten vorhalten und bearbeiten.
2. Nutzen sie die verschiedenen Möglichkeiten, die Sicherheitsoptionen ihres Betriebssystems, Ihres Web-Browsers und Ihres E-Mail-Programms anzupassen.
3. Geben Sie im Internet nicht freimütig Auskunft über Ihren Namen, Ihre Anschrift, Ihre E-Mail-Adresse und Weiteres. Dies gilt in erster Linie für Chats, Newsgruppen und Gewinnspiele.
4. Falls Sie sich häufiger in Chatrooms oder Newsgroups aufhalten, legen Sie sich eine zweite Mail-Adresse bei einem Freemailer zu und geben Sie z. B. in Newsgroups diese an.
5. Verwenden Sie vernünftige Paßwörter, die nicht im Duden stehen und mindestens 6 Zeichen lang sind (am besten eine Kombination aus Groß- und Klein-Buchstaben sowie Zahlen). Auf keinen Fall sollten Sie leicht zu erratende Passworte wie Ihren Namen, Ihr Geburtsdatum oder so sinnige Varianten wie "Passwort" oder "geheim" vergeben.
6. Speichern Sie keine Passwörter auf Ihrer Festplatte und geben Sie Ihre Kennwörter nicht an Dritte weiter.
7. Installieren Sie nur Programme, die Sie auch tatsächlich benutzen und schalten Sie nicht benötigte Funktionen ab.
8. Vorsicht bei dem Öffnen von E-Mail-Anhängen! Vor allem bei verdächtigen Dateiendungen wie *.vbs, *.com, *.exe, *.pif oder *.scr.
9. Größte Vorsicht bei Downloads von Programmen aus dem Internet! Laden Sie möglichst keine Programme von nicht vertrauenswürdigen Seiten herunter. Diese könnten Trojaner, Viren oder aktuell 0190-Dialer enthalten. Vor der Installation empfiehlt es sich, die Software einem Check mit dem Virenscanner zu unterziehen.
10. Nutzen Sie möglichst die aktuellste Browserversion, da dort bereits bekannte Sicherheitslücken früherer Versionen meist nicht mehr vorkommen.
11. Aktivieren Sie die interne WindowsXP-Firewall (Internet-Verbindungs-Firewall).
12. Nutzen Sie einen aktuellen Virenscanner und laden Sie regelmäßig die neusten Virensignaturen vom Hersteller herunter.
13. Sicherheitslöcher in Betriebssystem und Software können durch aktuelle Service Packs und Patches des Herstellers gestopft werden.
14. Schalten Sie im E-Mail-Programm das HTML-Format für Mails ab.
15. Nutzen Sie Verschlüsselung, falls Sie sensible Daten per E-Mail versenden.
16. Falls Sie persönliche Daten über das Internet weitergeben, achten Sie darauf, dass dies über eine gesicherte, verschlüsselte Verbindung passiert. Dies erkennen Sie daran, daß die URL statt mit http:// mit https:// beginnt.
17. Deaktivieren Sie im Browser und im E-Mail-Programm vor allem ActiveX und im Zweifelsfall auch JavaScript.
18. Machen Sie regelmäßig Sicherungskopien Ihrer Daten.
19. Erstellen Sie eine Notfallstartdiskette bzw. CD.

Überreicht durch: Entropia e.V., Steinstraße 23, 76133 Karlsruhe, http://www.entropia.de
Text vom Landesbeauftragten für den Datenschutz Bremen, http://www.datenschutz-bremen.de