Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: PRIVATE IT

Sichere private Nutzung des Internets

Ausgangslage

Viele nützliche und wichtige Dienstleistungen – wie Online-Banking, E-Commerce oder E-Government – werden heute über das Internet genutzt. Auch in Zukunft wird sich die Anzahl der angebotenen Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz neuer mobiler Endgeräte (Smartphones und Tablets), mit denen diese Dienstleistungen genutzt werden können. Personal Computer (PCs) mit verschiedenen Betriebssystemen, wie Apple Mac OS X, Microsoft Windows oder einer Linux-Variante, spielen derzeit jedoch noch die wichtigste Rolle.

Ziel

Die vorliegende BSI-Empfehlung bietet allgemeine Hilfestellungen für den Umgang mit Ihrer privaten Informationstechnik bei der Anschaffung und bei der alltäglichen Nutzung. Mit wenigen Maßnahmen können Sie zu einer weitgehend sicheren Nutzung von Dienstleistungen über das Internet beitragen, unabhängig vom verwendeten Betriebssystem. Für Maßnahmen, die spezifisch für Ihr verwendetes Betriebssystem sind, beachten Sie die entsprechenden BSI-Veröffentlichungen für den Einsatz von Microsoft Windows, Apple OS X Mountain Lion und Ubuntu Linux.

Bei der Anschaffung

Bereits bei der Anschaffung Ihrer Heim-IT gibt es wichtige Aspekte, die Sie für die Sicherheit im späteren Betrieb beachten sollten.

Internet-Provider

Die Auswahl eines geeigneten Internet-Providers sollte nicht nur vom Preis des Internetanschlusses abhängig sein, sondern auch andere Kriterien berücksichtigen. Es ist empfehlenswert, beispielsweise darauf zu achten, dass Ihr Anbieter seine Kunden aktiv vor Internet-Kriminalität zu schützen versucht. Insbesondere sollte Ihr Internet-Provider die Abwehr von Botnetzen – auch zu Ihrem eigenen Schutz – mit wirksamen Maßnahmen auf demselben Niveau betreiben wie Provider, die in der Anti-Botnet-Initiative zusammengeschlossen sind.

E-Mail-Provider

Neben der Nutzung von Angeboten im World Wide Web (WWW) ist eine der Hauptaufgaben von Internet-PCs der Empfang und Versand von E-Mails. Für diesen Zweck benötigen Sie einen geeigneten E-Mail-Provider.

Die Mindestanforderungen an einen E-Mail-Provider sind:

- Bereitstellung eines E-Mail-Virenfilters
- Schutz vor Spam-E-Mails
- Durchgehend verschlüsselter Zugang, unabhängig davon ob Sie per Internet-Browser oder E-Mail-Programm auf Ihr Postfach zugreifen; konkret bedeutet dies die Unterstützung der Protokolle HTTPS für Webmail sowie SMTPS und POP3S bzw. IMAPS für den Zugriff über ein E-Mail-Programm.

Diese Sicherheitsfunktionen sowie verschlüsselte Zugänge stellt z. B. Google bei Google Mail kostenlos zur Verfügung. Bei weit verbreiteten Anbietern wie z. B. GMX und Web.de sind die genannten Funktionalitäten ebenfalls verfügbar, jedoch oftmals erst in den kostenpflichtigen Varianten.

Router und WLAN

Für den Internet-Anschluss sollten Sie in jedem Fall einen Router nutzen. Im Gegensatz zu Modems (z. B. für DSL oder Kabel) sind bei Routern Firewall und Verschlüsselungsfunktionen integriert, die Sie aktivieren bzw. einstellen müssen. Ändern Sie unbedingt das voreingestellte Passwort für den Zugriff auf die Konfigurationsoberfläche des Routers.

Die meisten Router verfügen heute über die Möglichkeit, Ihre Geräte (wie z. B. Notebooks) drahtlos mit dem Internet zu verbinden (WLAN). Deaktivieren Sie die WLAN-Funktionalität, wenn Sie diese nicht benötigen.

Wenn Sie WLAN nutzen möchten, muss die Verbindung sicher verschlüsselt werden. Der aktuelle Verschlüsselungsstandard ist WPA2. Ändern Sie nach der Inbetriebnahme das voreingestellte WLAN-Passwort Ihres Routers. Dieses müssen Sie nur selten eingeben (jeweils bei der ersten Verbindung eines neuen Geräts mit dem Router), sodass Sie ohne besondere Komforteinbuße ein zufälliges, komplexes und langes Passwort wählen können. Notieren Sie sich dieses Passwort und bewahren Sie es an einem sicheren Ort und nicht im unmittelbaren räumlichen Umfeld Ihrer Geräte oder des Routers auf. Das WLAN-Passwort und das Passwort für die Konfigurationsoberfläche des Routers sollten sich auf jeden Fall unterscheiden. Es ist außerdem empfehlenswert, den Namen Ihres WLANs – auch als *SSID* bezeichnet – zu ändern. Der Name sollte keine Rückschlüsse auf den Betreiber des WLANs oder den Hersteller des Routers erlauben.

Neuer Personalausweis

Für die Nutzung der eID-Funktion (eID = elektronische Identität) des neuen Personalausweises (https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/personalausweis_node.html) benötigen Sie die Software *AusweisApp*. Diese finden Sie zum Download auf dem AusweisApp-Portal (https://www.ausweisapp.bund.de). Ebenso benötigen Sie ein zertifiziertes Lesegerät. Hinweise auf entsprechende Geräte finden Sie ebenfalls auf dem Portal der AusweisApp.

Informationen zum Thema „neuer Personalausweis“ finden Sie unter http://www.personalausweisportal.de und bei „BSI für Bürger“ (https://www.bsi-fuer-buerger.de/NeuerPersonalausweis).

Bei der täglichen Nutzung

Beachten Sie im täglichen Gebrauch die folgenden Ratschläge für einen sicheren Betrieb.

Überblick über die allgemeine IT-Sicherheitslage

Verschaffen Sie sich regelmäßig einen Überblick über die aktuelle IT-Sicherheitslage, z. B. über die Schwachstellenampel des BSI sowie durch ein kostenloses Abonnement der BSI-Meldungen des Bürger-CERT-Newsletters.

So werden Sie über aktuelle oder neuartige Angriffsmethoden informiert, wie z. B. Betrugsmaschen beim Kauf von Waren oder die betrügerische Erschleichung von Kreditkartendaten durch geschickt formulierte E-Mails.

Online-Banking

Setzen Sie beim Online-Banking ein sicheres, modernes Verfahren zur Freigabe von Überweisungen ein. Derzeit ist dies das ChipTAN-Verfahren, bei dem die Freigabe der Überweisung durch ein spezielles Lesegerät in Verbindung mit Ihrer Bankkarte erfolgt. Mindestens jedoch sollten Sie das mTAN-Verfahren einsetzen. Hier wird die Transaktionsnummer (TAN) zur Freigabe der Überweisung per SMS auf Ihr Mobiltelefon übermittelt. Wichtig dabei ist, dass die SMS nicht mit dem Smartphone empfangen wird, von dem aus auch das Bankgeschäft durchgeführt wird. Dies würde die Trennung der Kanäle Internetverbindung und Mobiltelefonieverbindung aufheben, auf der die Sicherheit basiert. Falls Ihre Bank eines der erwähnten Verfahren anbietet, sollten Sie auf den Einsatz papiergebundener TAN-Verfahren (z. B. TAN und iTAN) verzichten.

Kommunikation

Kommunikation über das Internet findet in den meisten Fällen per E-Mail statt. Gegenwärtig werden jedoch über 95 Prozent aller E-Mails unverschlüsselt versendet und können daher wie eine Postkarte von Unberechtigten abgefangen, mitgelesen und verändert werden. Bei höheren Anforderungen an die Sicherheit und Vertraulichkeit von E-Mails kann der Dienst De-Mail verwendet werden.

Der De-Mail-Postfach- und Versanddienst gewährleistet eine zuverlässige und vertrauliche Kommunikation. Durch spezielle Versand- und Eingangsbestätigungen wird die Kommunikation nachweisbar und nachvollziehbar. Zusätzlich werden die Nachrichten gemäß der gewählten Versandoptionen durch die De-Mail-Diensteanbieter gegen Veränderungen des Nachrichteninhalts und der sogenannten Metadaten (z. B. Absenderadresse, Versandzeit, Versandoptionen) geschützt.

Wenn Sie De-Mail nicht nutzen möchten, können Sie Ihre E-Mails auch mithilfe zusätzlicher Software selbst verschlüsseln und signieren, um individuell einen Schutz der Vertraulichkeit zu erreichen und die Authentizität und Integrität Ihrer E-Mails zu sichern. Die hierfür notwendigen Anwendungen wie z. B. Gpg4win für Microsoft Windows oder GPGTools für Apple OS X sind vielfach kostenfrei erhältlich bzw. in Linux-Distributionen wie Ubuntu bereits enthalten.

WLAN und Bluetooth

Deaktivieren Sie Funknetz-Dienste wie WLAN und Bluetooth, wenn Sie diese nicht benötigen, um Angriffe über diese Schnittstellen zu verhindern. Dies gilt insbesondere für den Betrieb an öffentlichen Orten, beispielsweise bei der Nutzung Ihres Notebooks in einem Café.

Verhaltensweisen im Internet und in Sozialen Netzwerken

Lassen Sie in der Online-Welt stets ein gesundes Misstrauen walten. Wenn Ihnen im Internet etwas merkwürdig erscheint, halten Sie inne und brechen Sie lieber einen Vorgang ab. Wenn Zweifel bestehen, geben Sie keine persönlichen Daten oder gar Ihre Kreditkartennummer an.

In Sozialen Netzwerken, wie z. B. Facebook oder Google+, sollten Sie sich immer so verhalten, wie Sie es auch in der realen Welt würden. Geben Sie nur Informationen preis, die Sie auch sonst einer beliebigen anderen Person mitteilen würden.

Konfigurieren Sie die Einstellungen zur Privatsphäre in Sozialen Netzwerken nach Ihren Bedürfnissen so restriktiv wie möglich. Fragen Sie regelmäßig Freunde oder Familienmitglieder, wie Sie aus deren Sicht im virtuellen Sozialen Netzwerk erscheinen. Versehentlich geteilte private Informationen werden in der Regel zunächst andere und nicht Sie selbst bemerken. Bitten Sie Ihr Umfeld, Sie darauf aufmerksam zu machen, wenn in Ihrem Profil im virtuellen Sozialen Netzwerk etwas unpassend erscheint oder ungewöhnliche Online-Kommunikation erfolgt, die unter Umständen auf Missbrauch oder Manipulation Ihres Profils schließen lässt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen IT-Themen. Kommentare und Hinweise können von Lesern an **mail@bsi-fuer-buerger.de** gesendet werden.