BSI - Online Banking - Ihre Software sicher einrichten

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/onlinebanking_node.html

Inhaltsverzeichnis

2. Ihre Software sicher einrichten

2.1 Sichere Einrichtung Ihrer Software

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungSoftware_node.html


Quelle: © *Sergey Nivens / Fotolia.com*

Was wäre die sichere Einrichtung Ihres Computers oder Ihres mobilen Gerätes, wenn zum Beispiel der Browser Sicherheitslücken aufweist, der immerhin die Schnittstelle zwischen Ihnen und dem Internet ist. Sich mit der Konfiguration des Browsers vertraut zu machen, ist ebenso empfehlenswert, wie diesen und andere Programme rasch zu aktualisieren, wenn Sicherheits-Updates - sogenannte Patches erscheinen.

Das BSI kann keine Empfehlungen aussprechen, welche Programme Sie nutzen sollten. Weil es aber immer wieder Fragen zur Sicherheit von Open Source Software gibt, die auch Freie Software genannt wird, haben wir für Sie eine Liste mit Antworten auf die wichtigsten Fragen zusammengestellt.

Schutzprogramme wie eine Firewall oder Browser-Erweiterungen gehören dagegen nicht zu der sicheren Einrichtung von Software und haben deshalb hier eine eigene Rubrik.

2.2 Der Browser

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/derbrowser_node.html

Der Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten und stellt somit eins der beliebtesten Ziele für Cyber-Angriffe dar. Hieraus ergibt sich ein besonders hohes Gefahrenpotenzial. Denn der Browser kann nicht nur die Informationen etwa einer Nachrichtenseite auf Ihrem Computer anzeigen, er kann auch der Weg sein, auf dem Schadsoftware wie Viren und Trojaner auf Ihr System gelangen.
Sie sollten deshalb wissen, wo Gefahren lauern und wie Sie sich am besten schützen können. In diesem Kapitel haben wir alle sicherheitsrelevanten Informationen rund um den Browser zusammengestellt.

Der erste Teil dieses Kapitels klärt über "Gefahren und Risiken" auf, die etwa in Aktiven Inhalten lauern.

Im Abschnitt "Sicherheitsmaßnahmen" erfahren Sie, welche Vorkehrungen Sie treffen sollten, damit das Surfen im Internet nicht zum Sicherheitsrisiko für Ihre Daten oder Ihren ganzen Computer wird.

2.2.1 Gefahren und Risiken

Ein Browser kommuniziert mit Servern, anderen Computern und Systemen, er empfängt und verschickt Daten. Er kann daher auch für den eigenen Computer schädliche Daten empfangen. Auf welchen Wegen das genau geschieht, wollen wir Ihnen in diesem Kapitel darstellen.

Eine gute Möglichkeit für Angreifer, über den Browser Schadcode zu installieren, stellen Sicherheitslücken im Browser selbst dar. Mehr zu diesem Thema lesen Sie im Text "Sicherheitslücken".

Aktive Inhalte sind kleine, ausführbare Programme innerhalb eines Browsers. Weil diese "ausführbar" sind, können sie von Angreifern missbraucht werden, um Schadcode auf Ihrem System installieren. Lesen Sie im Text "Aktive Inhalte", wie diese im Browser zum Sicherheitsrisiko werden können.

Im Kapitel "Browser-Entführung" erfahren Sie, wie Angreifer den Browser so manipulieren können, dass Sie nicht auf der von Ihnen gewünschten Webseite landen, sondern auf einer, die Schadcode enthält und eine Gefahr für Ihr System darstellt.

Nicht unmittelbar ein Sicherheitsrisiko, aber doch ein mögliches Datenschutzproblem stellen Cookies dar – kleine Dateien, die bestimmte Informationen über Ihren Besuch auf einer Webseite auf Ihrem Computer speichern. Bei einem erneuten Besuch auf dieser Webseite werden die auf Ihrem Computer gespeicherten Informationen ausgelesen. Mehr zum Thema gibt es im Artikel "Cookies".

▪ 2.2.1.1 Sicherheitslücken

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/GefahrenRisiken/Sicherheitsluecken/sicherheitsluecken_node.html

Die Hersteller von Browsern versuchen zwar ihre Programme so sicher wie möglich zu entwickeln, doch das gelingt niemals zu 100 Prozent. Browser können immer Sicherheitslücken enthalten, die von Angreifern ausgenutzt werden können. Um diese aufzuspüren, gibt es für die Angreifer zwei Strategien: Entweder warten sie darauf, dass der Hersteller ein Update (auch "Patch" genannt, dt. "Flicken") veröffentlicht, das die Sicherheitslücke schließt. Dann wissen die Angreifer, welche Schwachstelle im Browser sie ausnutzen können. Diese Vorgehensweise ist überlicherweise erfolgreich, denn viele Anwender sind nachlässig mit der Installation von Browser-Updates.
Oder die Angreifer suchen selbst nach Sicherheitslücken, über die sie in ein Computer-System eindringen können.

Sicherheitslücken können zum Beispiel für sogenannte Drive-by-Downloads ausgenutzt werden. Dabei verstecken Angreifer schädliche Programme auf Webseiten. Durch eine Sicherheitslücke lädt sich das Programm beim Besuch der Seite selbst auf den Rechner des Anwenders. Häufig wird derartige Schadsoftware verwendet, um Daten auszuspionieren oder Schaden auf dem Zielrechner zu verursachen.

▪ 2.2.1.2 Aktive Inhalte

Die Daten, die der Browser abruft, um daraus die anzuzeigende Webseite zusammenzusetzen, enthalten häufig nicht sichtbare Programmteile oder Skripte. Sie sind für verschiedene Funktionen wie animierte Menüs oder Videos zuständig und werden als "Aktive Inhalte" bezeichnet. Die bekanntesten sind Java, ActiveX-Controls, JavaScript/JScript und Flash/Silverlight.

An der im Browser angezeigten Webseite ist nicht erkennbar, welche Funktionen sich im einzelnen hinter den Aktiven Inhalten verbergen. Es könnte sich also auch mitunter um Schadprogramme handeln. Jede Art von Aktiven Inhalten hat ein unterschiedliches Schadpotenzial:

2.2.1.2.1 Java

Java-Programme, die im Rahmen einer Website ausgeführt werden, werden auch "Java-Applets" genannt. Durch Aufrufen der Webseite werden die Applets auf den PC heruntergeladen und ausgeführt. Die Java-Applets laufen also wie ein direkt auf dem Rechner installiertes Programm ab.
Java-Applets können normalerweise nicht ohne Ihre Erlaubnis auf lokale Daten zugreifen. Wenn ein betrügerisch veranlagter Seitenersteller sich Ihre Erlaubnis jedoch erschleicht oder in der Implementierung der Java Virtual Machine Fehler enthalten sind, kann trotz allem der uneingeschränkte Zugriff auf Ihren Rechner und Ihre Daten möglich werden.

2.2.1.2.2 ActiveX-Controls

ActiveX ist eine von Microsoft entwickelte Technik, die im Internet Explorer zum Einsatz kommt. Die ActiveX-Elemente, die als Aktiver Inhalt in Webseiten eingefügt werden können, werden ActiveX-Controls genannt. Sie werden z. B. verwendet für Videos und Musik, aber auch für komplexere Inhalte wie Aktienticker. Leider werden auch häufig Schadprogramme auf diesem Weg verbreitet.
Dies ist so einfach möglich, da es keine umfassenden Sicherheitsrichtlinien gibt. Es gibt zwar signierte ActiveX-Controls, doch die Signatur bestätigt letztlich nur, von wem das ActiveX-Control stammt. Läuft das ActiveX-Programm erst einmal, dann ist sein Funktionsumfang in keiner Weise eingeschränkt. Das ActiveX-Programm besitzt alle Rechte des angemeldeten Benutzers.

2.2.1.2.3 JavaScript/JScript

JavaScript ist eine an Java angelehnte Skriptsprache. Skriptsprache heißt dabei, dass es sich um eine Programmiersprache handelt, die beim Anwender im Textformat vorliegt und durch ein eigens dafür vorgesehenes "Übersetzungsprogramm" (Interpreter) ausgeführt wird. JavaScript wurde speziell für den Einsatz als Aktiver Inhalt in Webseiten von der Firma Netscape entwickelt. JavaScript eignet sich beispielsweise zur Überprüfung von Formulareingaben innerhalb von Webseiten.
Wie die Java-Applets kommen auch die in JavaScript geschriebenen Aktiven Inhalte mehr oder weniger ungefragt auf Ihren Rechner. An der angezeigten Webseite ist nicht erkennbar, was sich so alles dahinter verbirgt. Hierdurch entsteht für den Anwender ein unüberschaubares Risiko. Schließlich sind auch bei JavaScript Fehler in der Implementierung nicht ausgeschlossen.
In der JScript genannten Variante von JavaScript, die Microsoft für den Internet Explorer entwickelt hat, gibt es Funktionen, die missbräuchlich eingesetzt einen großen Schaden auf dem Rechner des Anwenders verursachen können. So gibt es unter JScript beispielsweise die Möglichkeit, ActiveX-Controls anzusprechen, die einmal auf den Rechner geladen die gleichen Rechte wie ein lokal installiertes Programm besitzen.

2.2.1.2.4 Flash/Silverlight

Über die von Adobe erstellte Software "Flash Player" wie auch über "Silverlight" von Microsoft können interaktive Inhalte und Anwendungen (z. B. interaktive Präsentationen, Spiele oder komplette Webseiten) angezeigt werden. Da Flash- und Silverlight-Inhalte über ein eigenes Plugin wiedergegeben werden, können diese alleine schon Sicherheitslücken enthalten, durch die Ihr Rechner angegriffen werden und Schadsoftware installiert werden könnte. Ebenso könnten diese Sicherheitslücken durch Angreifer ausgenutzt werden, um auf Ihre Webcam oder das Mikrofon Ihres Computers zugreifen zu können.

▪ 2.2.1.3 Browser-Entführung

Mit dem Begriff Browser-Hijacking (dt.: Browser-Entführung) ist die Umleitung von Browser-Anfragen auf fremde Internetseiten gemeint. Statt auf Ihrer voreingestellten Startseite oder der eingegebenen Web-Adresse landen Sie also woanders, meist auf Werbeseiten – Ihr Browser wird dorthin entführt.

Verantwortlich für eine Browser-Entführung sind kleine Programme, die den Browser unter ihre Kontrolle bringen. Sie richten zwar keinen direkten Schaden an, sind aber lästig und lassen sich nur mit Mühe wieder entfernen. Auch das Suchfeld im Browser wird für solche Zwecke missbraucht und führt dann nicht zum gewünschten Suchergebnis, sondern ebenfalls auf Werbeseiten. Zusätzlich können Ihre Favoriten beziehungsweise Lesezeichen/Bookmarks verändert oder ergänzt werden.

Zunutze machen sich die Browser-Entführer Schwachstellen im Betriebssystem oder in Anwendungen. Dabei gibt es eine Reihe von Möglichkeiten für Browser-Entführer, sich im System hartnäckig festzusetzen.

Beim Microsoft Internet Explorer können Angreifer beispielsweise sogenannte Browser-Helper-Objekte (BHO) nutzen. Diese ausführbaren Programme dienen eigentlich zur Erweiterung der Browserfunktionen des Internet Explorers, z. B. um PDF-Dateien direkt im Browser betrachten zu können (Adobe Reader-Plug-in). Böswillige BHOs können unerkannt auf Ihrem Rechner installiert werden. Die BHOs haben damit Zugriff auf alle Funktionen des Internet Explorers und können so das Verhalten des Browsers manipulieren.
Doch auch in anderen Browsern wie dem Mozilla Firefox, können die Erweiterungen (auch Add-on genannt) schädliche Software enthalten.

▪ 2.2.1.4 Cookies

Cookies sind kleine Dateien, die nach dem Besuch einer Internetseite auf dem PC oder Smartphone abgelegt werden. In dieser Datei werden Informationen gespeichert, die im Zusammenhang mit der jeweiligen besuchten Internetseite stehen. Sie merken das z. B. daran, dass Sie beim Ausfüllen des Online-Bestellzettels Daten, die sie einmal eingetragen haben, nicht immer wieder eintippen müssen. In den Browseroptionen können Sie einstellen, ob und von welcher Webseite Cookies gespeichert werden und wann diese gelöscht werden sollen.

Weil Cookies keine ausführbaren Programme sind, stellen sie kein direktes Sicherheitsrisiko dar. Dennoch sind sie nicht unproblematisch: Cookies werden auch eingesetzt, um Internetseiten auf Ihre persönlichen Wünsche zuzuschneiden. Problematisch ist, dass hierbei ein sehr genaues Nutzerprofil angelegt werden kann. Unternehmen setzen solche Cookies zum Beispiel ein, um passende Werbung anzuzeigen.

2.2.1.4.1 Zwei Arten von Cookies

Es sind zwei Arten von Cookies zu unterscheiden: Die dauerhaften Cookies und die Session-Cookies. **Dauerhafte Cookies** bleiben über Monate oder gar Jahre auf Ihrem Computer – zumindest dann, wenn sie nicht automatisch oder manuell gelöscht werden. Die **Session-Cookies** dagegen werden automatisch immer dann gelöscht, wenn der Browser geschlossen wird. Diese nutzten etwa Banken für das Online-Banking. Ein Sicherheitsrisiko stellen diese Cookies nicht dar. Problematisch sind die dauerhaften Cookies. Denn diese können über eine lange Zeit das Nutzungsverhalten des Anwenders protokollieren – etwa, nach welchen Produkten in welchen Online-Shops er sucht.

Ein weiteres Risiko bergen Cookies auf öffentlich zugänglichen Computern. Manche soziale Netzwerke sorgen durch Cookies dafür, dass Anwender angemeldet bleiben, wenn sie nur den Browser geschlossen, sich aber nicht aktiv ausgeloggt haben. Der nächste Benutzer des öffentlichen Computers kann dann im Profil des vorherigen Anwenders stöbern und gegebenenfalls Schaden anrichten

2.2.1.4.2 Cookies von Drittanbietern

Generell gilt, dass nur die Webseite die Cookies auslesen darf, die sie selbst gesetzt hat – Online-Shop A darf also nicht den Cookie von Online-Shop B auslesen. Allerdings gibt es auch noch sogenannte Drittanbieter, also zum Beispiel Werbeagenturen, die Werbebanner auf verschiedenen Webseiten platzieren. Solche Werbebanner setzen manchmal eigene Cookies. Wenn nun ein Anwender drei verschiedene Webseiten mit dem (zufällig) selben Werbebanner-Cookie besucht hat, kann die Werbeagentur theoretisch über ihren Cookie auslesen, welche drei Webseiten das waren. Sie enthält damit ein recht umfassendes Portfolio über das Surfverhalten einer Person. Cookies von Drittanbietern werden daher von Datenschützern als problematisch bewertet.

2.3 Sicherheitsmaßnahmen

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/sicherheitsmassnahmen_node.html

Einen sicheren Browser kann es nur in einer sicheren Umgebung geben. Daher gelten folgende allgemeine Empfehlungen:

2.3.1 Basisschutz

Installieren Sie eine aktuelle Firewall auf Ihrem Rechner. Verwenden Sie einen Virenscanner und achten Sie darauf, dass dieser stets auf dem neuesten Stand ist und aktuelle Virensignaturen verwendet (siehe auch: "Basisschutz für den Computer").

- **2.3.1.1 Halten Sie Ihr System aktuell**

Installieren Sie alle Updates sofort nach ihrer Veröffentlichung, sowohl die für Ihren Browser, als auch für alle Erweiterungen und natürlich Ihr Betriebssystem. Verwenden Sie stets die neuste Version Ihres Browsers. Heute kommunizieren aber nicht nur Ihr Browser und E-Mail-Programm sowie deren Erweiterungen (Add-ons, Plug-ins) mit dem Internet. Auch sollte sämtliche Anwendersoftware aktuell gehalten werden, da zum Beispiel auch PDFs oder Office-Dokumente über dynamische Inhalte und Makros eine Verbindung zum Internet herstellen können.

Hilfestellung für mehr Sicherheit im Browser selbst erhalten Sie auf den folgenden Seiten. Zunächst finden Sie einige Konfigurationshinweise (Machen Sie Ihren Browser sicher).

Wenn über den Browser persönliche Daten, Passwörter oder Zahlungsinformationen gesendet werden, ist eine verschlüsselte Verbindung wichtig. Wie Browser eine sichere Verbindung signalisieren, erfahren Sie unter Verschlüsselung/Zertifikate.

Java ist eine objektorientierte Programmiersprache, die die Möglichkeit bietet, Programme plattformübergreifend direkt im Browser einzubinden und auszuführen. Java genießt in der IT-Welt eine hohe Verbreitung, was sie jedoch gleichzeitig zu einem beliebten Ziel für Angriffe und Missbrauch macht. Das BSI empfiehlt das Ausführen von Java-Anwendungen im Browser zu deaktivieren. Mehr hierzu erfahren Sie in dem Text Sicherheit von Java.

Wie Sie Ihren Browser so einstellen, dass über Cookies möglichst keine persönlichen Profile erstellt werden können, ist im Text Cookies vermeiden zusammengefasst.

Schließlich folgt noch der Hinweis, dass auch beim Internetsurfen der gesunde Menschenverstand (Surfen Sie mit gesundem Menschenverstand) zu mehr Sicherheit beiträgt.

2.3.2 Machen Sie Ihren Browser sicher

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/SicherheitsCheck/sicherheitscheck_node.html;jsessionid=07E3758559EFB3A68BCF8B23E0FC05EB.2_cid351

Die ideale Browsereinstellung für alle Surfer gibt es nicht. Wenn eine Internetseite z. B. nur mit Adobe Flash funktioniert, müssen Sie abwägen, ob Sie zugunsten der Sicherheit ganz darauf verzichten oder das damit verbundene Risiko in Kauf nehmen.

▪ 2.3.2.1 Generelle Empfehlungen:

Verwenden Sie nach Möglichkeit einen Browser mit Sandbox-Technologie wie zum Beispiel Google Chrome und einer guten Versorgung mit Sicherheitsupdates. Verzichten Sie auf die Nutzung Aktiver Inhalte, soweit Sie diese nicht benötigen – dies gilt insbesondere für Techniken wie Java, die durch zusätzliche Plugins bereitgestellt werden und nicht bereits durch den Browser direkt unterstützt werden. Wenn Sie solche Aktiven Inhalte nutzen müssen, schalten Sie sie generell aus und aktivieren diese nur bei vertrauenswürdigen Webseiten. Aktivieren Sie die in allen gängigen Browsern integrierten Mechanismen zum Phishing- und Malware-Schutz.

▪ 2.3.2.2 Sicherheitseinstellungen der gängigen Browser

Hinweise und Anleitungen zu Sicherheitseinstellungen der gängigen Browser finden Sie auf den jeweiligen Hilfe-Seiten:

2.3.2.2.1 Firefox:

- Sicherheitseinstellungen: http://support.mozilla.org/de/kb/Einstellungen-Fenster%20-%20Sicherheits-Abschnitt

Empfehlung: Verwenden Sie die Standard-Einstellungen von Firefox. Deaktivieren Sie die Option "Passwörter speichern". Falls Sie Passwörter im Browser speichern wollen, verwenden Sie unbedingt ein Master-Passwort (Beachten Sie die Hinweise für ein sicheres Passwort).

2.3.2.2.2 Internet Explorer:

- Sicherheitseinstellungen: http://windows.microsoft.com/de-DE/internet-explorer/ie-security-privacy-settings
- Blockieren aktiver Inhalte im IE 9: http://windows.microsoft.com/de-AT/windows7/How-to-use-Tracking-Protection-and-ActiveX-Filtering

Empfehlung: Blockieren Sie die ActiveX-Steuerelemente. Verwenden Sie die neueste Version des Internet Explorers, die für Ihre Windows-Version verfügbar ist.

2.3.2.2.3 Chrome:

- Sicherheitseinstellungen: http://support.google.com/chrome/?hl=de#topic=14666&rd=1
- Blockieren Aktiver Inhalte in Google Chrome: http://support.google.com/chrome/bin/answer.py?hl=de&answer=142064

Empfehlung: Wählen Sie unter "Plugins blockieren" die Funktion "Click-to-Play".

2.3.2.2.4 Opera:

- Sicherheitseinstellungen http://help.opera.com/
- Guide to security and privacy in Opera http://de.opera.com/browser/tutorials/security/

2.3.2.2.5 Safari:

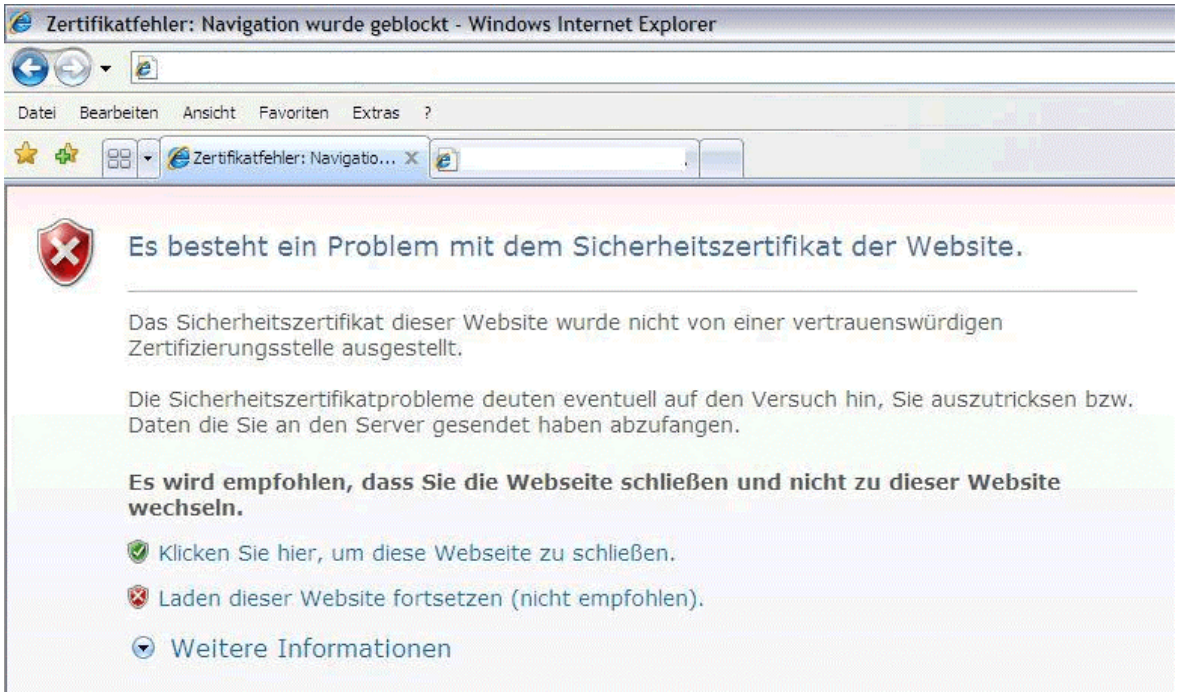
Auf der Internetseite von Apple gibt es keine Zusatzinformationen zu den Sicherheitseinstellungen des Browsers. Das Online-Portal "Verbraucher Sicher online" hat eine Anleitung "Sicher surfen mit dem Browser Safari" erstellt.

2.3.3 Verschlüsselung/Zertifikate

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/Verschluesselung/verschluesselung_node.html

Bestimmte Daten sollten beim Surfen verschlüsselt übertragen werden, etwa Kreditkarten-Daten beim Online-Shopping. Der Browser verwendet dazu eine Technik, die SSL/TLS-Protokoll genannt wird. Sie baut eine sichere Netzverbindung zwischen Webseite und Ihrem Rechner auf.
SSL steht für "Secure Socket Layer". Inzwischen wird das Protokoll unter dem Namen "TLS" (Transport Layer Security) weiter entwickelt. Die SSL/TLS-Technik identifiziert die Internetseite und gewährleistet, dass Daten während der Übertragung nicht gelesen oder manipuliert werden können. Das SSL- bzw. TLS-Protokoll wird heute von allen gängigen Browsern unterstützt.

Dass ein Browser eine verschlüsselte Verbindung mit der aufgerufenen Internetseite aufgebaut hat, ist daran zu erkennen, dass am Beginn der Webseiten-Adresse dem "**http**" ein "**s**" (für: "secure", dt.: "sicher") angehängt wurde. Dann lautet die Internetadresse zum Beispiel: https://www.bsi-fuer-buerger.de. Bei sensiblen Online-Transaktionen, wie Banking, Shopping etc. solllte die Website über eine solche https-Adresse aufgerufen werden.



Bei jedem Aufruf einer https-Adresse prüft der Browser, ob der Anbieter der Internetseite ein gültiges Zertifikat vorweisen kann. Kann er das nicht, dann warnt der Browser mit einer Nachricht. Bei einer solchen oder ähnlichen Warnung des Browsers sollten Sie nicht auf der jeweiligen Webseite weitersurfen.

Neben diesem Warnhinweis gibt es noch ein zweites Sicherheitsmerkmal, auf das Sie achten sollten: die Stärke des Zertifikats. Diese wird Ihnen in verschiedenen Browsern auf unterschiedliche Art angezeigt. Im Internet Explorer, Mozilla Firefox oder Google Chrome ändert sich die Farbe des Feldes oder der Schrift vor beziehungsweise hinter der Adresszeile in grün – das steht für die höchste

Zertifikatstufe.
Hier ein Beispiel:

Welche Browser, auf welche Weise und in welcher Farbe die unterschiedlichen Zertifikatstufen anzeigen, ist auf den jeweiligen Informationsseiten zusammengefasst. Beachten Sie generell die Regel: Bei sensiblen Transaktionen muss die höchste Zertifikatstufe verwendet werden. Im Zweifelsfall brechen Sie Ihr Vorhaben ab. Je nach verwendetem Browser (bzw. Betriebssystem) finden Sie in den "Einstellungen" eine Liste der gültigen Zertifizierungsstellen.

- Mozilla Firefox: Schaltfläche zur Webseitenidentität
- Internet Explorer: Was bedeuten die verschiedenen Farben der Sicherheitsstatusleiste?
- Chrome: Identität der Webseite
- Opera (auf englisch): Security Information
- Safari: Verwenden von Webseiten-Verschlüsselung

2.3.3.1 Video für z.B. interne Sensibilisierungsmaßnahmen in einer höheren Auflösung.

- Download des Videos zum Thema "Sichere Datenübertragung"

https://download.gsb.bund.de/BSI/BSIfB/Sichere_Datenuebertragung_mp4.zip

2.3.4 Sicherheit von Java. Empfehlungen zur sicheren Nutzung

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/Java/java_node.html;jsessionid=BDB4DEB704F9FF97128BF99E81D2EBCB.1_cid369

Java ist eine objektorientierte Programmiersprache, die sich aufgrund der Möglichkeit, Programme plattformübergreifend direkt im Browser einzubinden und auszuführen, schnell großer Beliebtheit erfreute und heute in der IT-Welt weit verbreitet ist.

Neben den Entwicklungskomponenten wird unter dem Begriff Java meist die Laufzeitumgebung (Java Runtime Environment, JRE) verstanden. Sie ist die Voraussetzung, dass Programme wie Open-Office/LibreOffice oder die AusweisApp und Applets ausgeführt werden können.

Weiterführende Informationen zu den Grundlagen sowie dem Sicherheitskonzept von Java finden Sie hier Sicherheit von Java (PDF, 157KB).

Java Applets und Java Web Start Applikationen werden zur Erhöhung der Sicherheit innerhalb einer sogenannten Sandbox (engl. übersetzt: Sandkasten) ausgeführt. Diese Sandbox hat die Aufgabe, den Code vom Rest des Systems abzukapseln und somit risikoreiche Operationen, z. B. das Schreiben auf der Festplatte, zu unterbinden. Leider gelingt es Angreifern durch das Ausnutzen von Implementierungsfehlern in der Java-Laufzeitumgebung immer wieder, das Sicherheitskonzept zu umgehen.

Aus diesem Grund empfiehlt das BSI, das Ausführen von Java-Anwendungen im Browser zu deaktivieren. Hilfestellung zu diesem Thema erhalten Sie unter den Java Sicherheitsempfehlungen.

Aktivieren Sie das Ausführen von Java im Browser gezielt nur dann, wenn Sie die Java-Inhalte tatsächlich benötigen, z. B. wenn Sie ElsterOnline (Erstellung der elektronischen Steuererklärung) verwenden möchten. Das BSI empfiehlt nach dem Zwei-Browser-Prinzip zu verfahren.

- Deaktivieren Sie die Java-Inhalte in Ihrem Standardbrowser.
- Installieren Sie einen zweiten Browser, in dem die Ausführung von Java-Inhalten erlaubt wird.

Weitere Hilfestellungen zur Auswahl und Absicherung eines Browsers.

Um ein grundlegendes Sicherheitsniveau erreichen zu können, überprüfen Sie die folgenden Sicherheitseinstellungen von Java.

▪ 2.3.4.1 Java Sicherheitsempfehlungen

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/Java/Java_Sicherheistempfehlungen/java_sicherheitsempfehlungen_node.html

Java Applets und Java Web Start Applikationen werden zur Erhöhung der Sicherheit innerhalb einer sogenannte *Sandbox* (engl. übersetzt: Sandkasten) ausgeführt. Diese Sandbox hat die Aufgabe, den Code vom Rest des Systems abzukapseln und somit risikoreiche Operationen, z. B. das Schreiben auf der Festplatte, zu unterbinden. Leider gelingt es Angreifern durch Ausnutzung von Implementierungsfehlern in der Java-Laufzeitumgebung immer wieder, dieses Sicherheitskonzept zu umgehen.

Aus diesem Grund empfiehlt das BSI, das Ausführen von Java-Anwendungen im Browser zu deaktivieren.

Aktivieren Sie das Ausführen von Java im Browser gezielt nur dann, wenn Sie die Java-Inhalte tatsächlichbenötigen, z. B. wenn Sie ElsterOnline (elektronische Steuererklärung) verwenden möchten. In diesem Fall empfiehlt das BSI, nach dem Zwei-Browser-Prinzip zu verfahren. Deaktivieren Sie die Java-Inhalte in Ihrem Standardbrowser und installieren Sie einen zweiten, den Sie nur für diesen Zweck verwenden. Weitere Hilfestellungen zur Auswahl und Absicherung eines Browsers.

Handlungsempfehlung

2.3.4.1.1 Die Ausführung von Java-Inhalte für *alle verwendeten* Browser deaktivieren

Die Deaktivierung erfolgt über das *Java Control Panel,* das Sie bei den unterschiedlichen Betriebssystemen hier finden:

- *Windows:* http://www.java.com/de/download/help/disable_browser.xml
- *Mac OS:* http://www.java.com/de/download/help/mac_controlpanel.xml
- *Linux*
  - Sun/OracleJava: Mit dem Befehl javaws -viewer über die Konsole
  - OpenJDK stellt das Java Control Panel nicht zur Verfügung

2.3.4.1.2 Die Ausführung von Java-Inhalten *in einem* Webbrowser deaktivieren

Sollten Sie nach dem Zwei-Browser-Prinzip verfahren und mehrere Browser nutzen, deaktivieren Sie die Ausführung von Java-Inhalten in Ihrem Standardbrowser. Auf der Seite von Java finden Sie hierzu eine Anleitung für **Internet Explorer, Firefox, Chrome und Safari**.

Die Deaktivierung von Java-Inhalten in ***Opera*** erfolgt über das Opera-Menü.
Wählen Sie "Einstellungen" aus und wechseln Sie zum Reiter "Erweitert". Unter dem Eintrag "Inhalte" finden Sie die Option "Plug-In aktivieren". Entfernen Sie dort das Häkchen.

Hinweis: Bitte beachten Sie, dass Mozilla das Java Plug-In für alle Plattformen aufgrund des erhöhten Risikos deaktiviert hat. Weitere Informationen erhalten Sie unter "Das Java-Plugin mit Firefox nutzen".

Stellen Sie sicher, dass Java auf Ihrem Computer sicher konfiguriert ist (siehe Java Konfiguration).

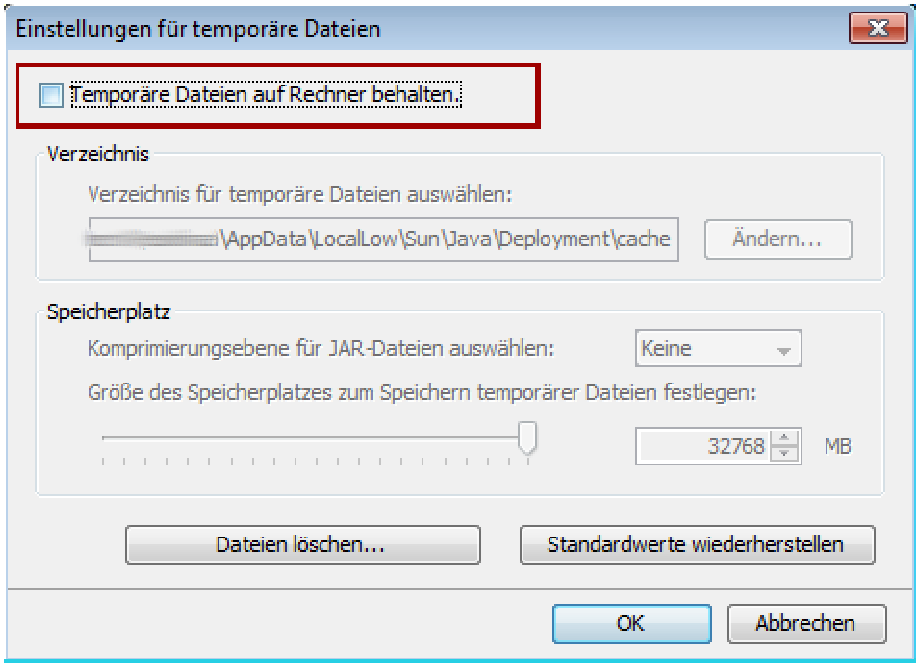
2.3.4.2 Konfiguration der Sicherheitseinstellungen von Java

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/Java/Java_Konfiguration/java_konfiguration_node.html

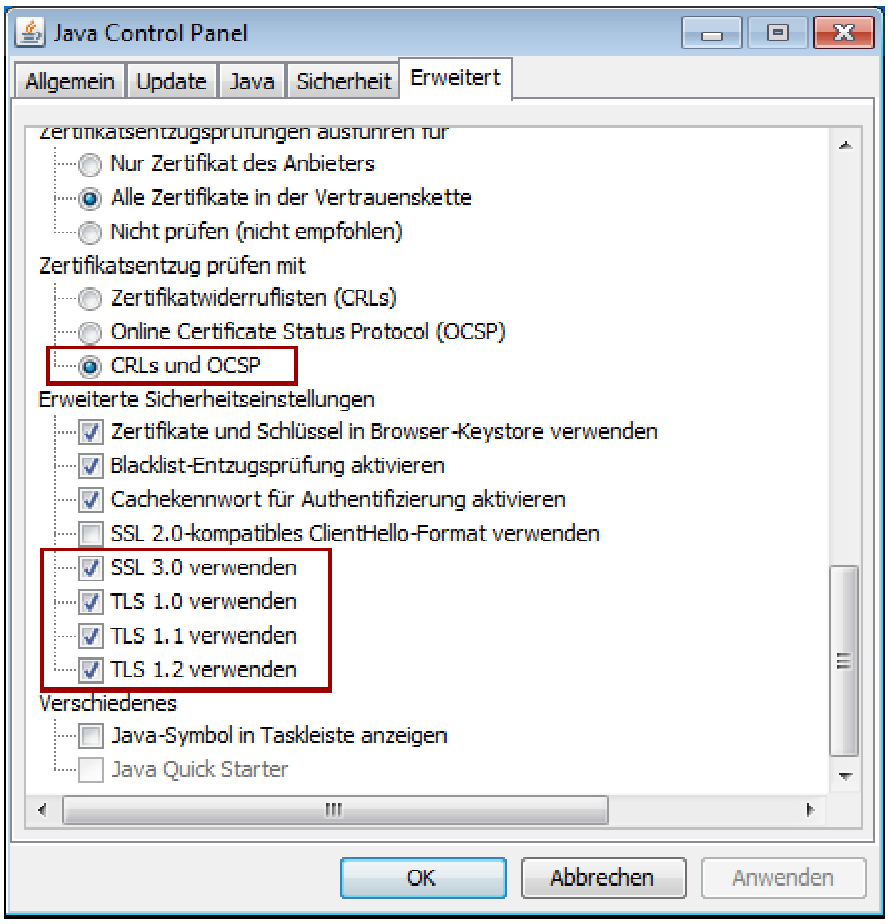
Die Sicherheitseinstellungen von Java werden im Java Control Panel vorgenommen. Wo finde ich das Java Control Panel?

2.3.4.2.1 Java-Cache leeren

Im Java-Cache werden verwendete Java-Anwendungen oder Java-Inhalte, die von besuchten Webseiten stammen, zwischengespeichert. Dadurch soll erreicht werden, dass beim erneuten Aufruf diese Ressourcen schneller geladen werden können. Dieser Zeitgewinn ist jedoch minimal. Das BSI empfiehlt das Leeren des Caches. Das Leeren bewirkt, dass der Browser eine neue Version der besuchten Webseiten oder verwendeten Java-Anwendungen herunterlädt. Des Weiteren werden Informationen über Ihr Surfverhalten gelöscht, was dem Schutz Ihrer Privatsphäre dient.
Das regelmäßige Leeren des Java-Caches erreichen Sie im Java Control Panel über den Reiter *"Allgemein"*. Wählen Sie die Option *"Einstellungen für temporäre Dateien"* aus und **deaktivieren** Sie anschließend das Kontrollkästchen *"Temporäte Dateien auf Rechner behalten"*.



Bestätigen Sie mit "OK" und wechseln Sie zum Reiter "Erweitert". Die mit rot markierten Sicherheitseinstellungen werden vom BSI empfohlen. Schalten Sie diese ggf. manuell ein.



2.3.4.2.2 Click-to-Play: Ausführung von Java-Inhalten im Browser

Click-To-Play ist eine weitere Einstellungsmöglichkeit, um die Gefahren, die durch automatisches Ausführen von Java-Inhalten im Browser ausgehen, zu minimieren, d.h., die Java-Inhalte werden erst nach einer Bestätigung seitens des Nutzers ausgeführt. Diese wird standardmäßig von aktuellen Browsern unterstützt und ist in den Voreinstellungen nicht aktiviert. Das BSI empfiehlt, diese Option zu aktivieren. Das Vorgehen dabei ist vom Browser abhängig:

Mozilla Firefox

Tippen Sie in der Adresszeile des Browsers **about:config** ein. Bestätigen Sie die folgende Meldung. Suchen Sie nach dem Eintrag **plugins.click_to_play**. Klicken Sie doppelt darauf, sodass der Wert auf **true** gesetzt wird.

Google Chrome

Chrome Menü > Einstellungen > Erweiterte Einstellungen anzeigen... > Datenschutz > Inhaltseinstellungen > Plug-ins > Aktivieren Sie die Option **"Click-to-Play"**.

Internet Explorer

Ab Version 10 kommt der Browser auch ohne Add-Ons aus. Hinweise zum vom Microsoft empfohlenen Vorgehen.

Opera

Opera Menü > Einstellungen > Einstellungen > Reiter "Erweitert" auswählen > Inhalte > Aktivieren Sie die Option "Plug-ins nur auf Anforderung“ > Bestätigen Sie mit OK.

Weitere Hinweise

Beachten Sie bei der Ausführung von Java-Inhalten im Browser die Hinweise von Oracle, die unter folgendem Link zu finden sind.

Das BSI empfiehlt, das Ausführen von Java-Inhalten, die gar nicht oder lediglich von unbekannten Herstellern signiert sind, abzubrechen.

2.3.5 Cookies vermeiden

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/Cookies/cookies_node.html

Es gibt verschiedene Möglichkeiten, Cookies in Browsern zuzulassen oder zu sperren. Hier führen wir einige auf. Bitte beachten Sie: Nicht jeder Browser bietet alle Möglichkeiten. (Details zu den Browsern finden Sie auf den jeweiligen Hilfe-Seiten, die unten verlinkt sind.)

- Sie können in den meisten Browsern einstellen, dass dauerhafte Cookies automatisch nach jedem Schließen des Browsers gelöscht werden (Session-Cookies werden immer automatisch gelöscht). Datenschutzprobleme fallen damit weg, ebenfalls das Risiko, dass der Nachfolge-Nutzer im Profil des Vorgängers angemeldet ist.
- Sie lassen dauerhafte Cookies prinzipiell zu, stellen den Browser aber so ein, dass sie erst nach Rückfrage gespeichert werden.
- Sie sperren dauerhafte Cookies, legen auf einer Liste aber Ausnahmen von Webseiten fest, die dauerhafte Cookies anlegen dürfen.
- Sie lassen dauerhafte Cookies prinzipiell zu, legen auf einer Liste aber Ausnahmen von Webseiten fest, die keine dauerhaften Cookies auf Ihrem Computer anlegen dürfen.

2.3.5.1 Hilfe-Seiten der Browser-Hersteller zu Cookies:

- Firefox: Cookies erlauben und ablehnen
  Empfehlung: Cookies akzeptieren und nur so lange behalten, bis Firefox geschlossen wird.
- Internet Explorer: Verwalten von Cookies im Internet Explorer 9
  Empfehlung: Führen Sie die Schritte unter "So können Sie alle Cookies blockieren oder zulassen" aus und stellen Sie den Regler auf "Hoch".
- Chrome: Cookies und Websitedaten verwalten
  Empfehlung: Wählen Sie die Option "Lokale Daten nach Beenden des Browsers löschen"
- Opera: Cookies-Einstellungen
  Empfehlung: Wählen Sie die Option "Neue Cookies beim Beenden von Opera löschen"
- Safari: Manage Cookies (Seite auf englisch)

2.4 E-Mail

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/E-Mail/E-Mail_node.html

Für die sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. Viele E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (HTTPS) zum Postfach zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die Verschlüsselung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen aktuellen und verbreiteten E-Mail-Client auswählen und diesen sicher konfigurieren, um z.B ein zusätzliches Einfallstor zur Ausführung von Schadcode auf Ihrem Rechner auszuschließen.

- Achten Sie bei der Nutzung von E-Mail-Programmen darauf, dass die Übertragungsprotokolle (POP3S, IMAPS, SMTPS) verwendet werden.
- Verzichten Sie auf die Darstellung und Erzeugung von E-Mails im HTML-Format.
- Deaktivieren Sie die Anzeige von externen Inhalten – beispielsweise Bilder in HTML-E-Mails.

2.5 Apps auf mobilen Geräten

Hüten Sie Ihr Smartphone besser als Ihren Schlüsselbund – dieser Tipp gilt erst recht, wenn Sie Ihr E-Mail-Postfach eingebunden haben oder Apps installiert sind. Denn dadurch bekommt das Smartphone die Funktion eines Generalschlüssels: Je nach installierter Software und gespeicherten Daten bietet es Zugang zu privaten und geschäftlichen Informationen – zu Fotos, Dokumenten, Passwörtern und vielem mehr.

Doch selbst wenn nur Sie als rechtmäßiger Besitzer Zugriff auf Ihr Smartphone haben, kommen beim täglichen Umgang verschiedene Parteien ins Spiel, denen Sie Ihre Datenschätze öffnen: Anwender müssen nicht nur dem Hersteller des Gerätes Vertrauen entgegenbringen, sondern auch den Herausgebern und Programmierern der Apps. Dritter Beteiligter ist der Betreiber des Netzes, über das Daten ausgetauscht werden. Auch ihm müssen Anwender vertrauen können, bevor sie Apps herunterladen und Daten speichern oder versenden. Erst wenn Sie allen Beteiligten vertrauen können, ist das Arbeiten mit Apps und persönlichen Daten empfehlenswert.

Die Gefahren von Apps sind vielfältig: Sie können nicht nur gespeicherte Daten in fremde Hände geben, sondern auch hohe Kosten verursachen. Einige bösartige Apps funktionieren wie die in vergangenen Zeiten von analogen Einwahlmodems verbreiteten Dialer auf dem PC: Sie bauen, ohne dass der Anwender es bemerkt, teure Telefonverbindungen auf oder versenden kostenintensive SMS, sogenannte Premium-SMS. Wieder andere bösartige Apps können Anwender dauerhaft überwachen, etwa indem sie regelmäßig Positionsdaten oder Passwörter übermitteln.

2.5.1 App-Sicherheitstipps

Installation

- Installieren Sie nur die Apps, die Sie tatsächlich benötigen. Jede zusätzliche App stellt zunächst ein zusätzliches Sicherheitsrisiko dar, selbst wenn es sich um ein seriöses Angebot handelt. Praktisch jede Software enthält Sicherheitslücken, Gerade bei kostenlosen Apps handeln Sie sich auch schnell potenziell unerwünschte Programme (PUP) wie falschen Antiviren-Schutz oder Adware ein. Der fragwürdige Zweck von Adware ist, Werbung einzublenden.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen – etwa den im Smartphone voreingestellten App-Stores und Markets der Hersteller.
- Prüfen Sie, auf welche Funktionen die App Rechte beansprucht. Je nach Betriebssystem können Sie vor der Installation einer App sehen, welche Rechte die Anwendung nach der Installation erhält. Achten Sie darauf, dass Apps nur auf die Smartphone-Funktionen zugreifen können, die für den Anwendungszweck nötig und plausibel sind. So ist Skepsis angebracht, wenn etwa eine Anwendung zum Speichern von Notizen auf die SMS-Funktion zugreifen will. Hier müssen Sie kritisch prüfen, ob Sie die Berechtigungen annehmen möchten, denn es gilt, alle Berechtigungen zu bestätigen oder die App nicht zu installieren. Weitere Informationen zur Bestätigung von App-Rechten unter Android finden Sie hier.
- Wenn Sie unsicher sind, ob die App vertrauenswürdig ist, hilft meist schon eine kurze Suche im Internet. Hier wird zeitnah informiert, wenn eine App Schadsoftware beinhaltet.
- Vorsicht bei Schnäppchen: Populäre Apps, vor allem Spiele, werden nachgeahmt. Die Nachahmer bieten die Apps billiger oder kostenlos an, bauen aber mitunter schädliche Funktionen in die Apps ein oder locken mit kostenpflichtigen "Extra-Leveln".

Aktualisierung

- Überprüfen Sie regelmäßig, ob Updates für Apps und Betriebssystem zur Verfügung stehen und installieren Sie diese möglichst umgehend.
- Seien Sie nicht nur bei der Installation neuer Apps, sondern auch bei Updates vorsichtig. Updates können vom Herausgeber genutzt werden, um eine App, der Sie nach einer gewissen Benutzungszeit vertrauen, mit zusätzlichen Zugriffrechten auszustatten. Verzichten Sie daher auf automatische Updates von Apps und installieren Sie die Updates manuell. Dann haben Sie je nach Betriebssystem die Möglichkeit sich die Rechte erneut anzeigen zu lassen.

Gebrauch

- Beobachten Sie die Statusleiste auf dem Smartphone-Bildschirm. An den Symbolen können Sie erkennen, wenn eine App Ortungsdaten sammelt oder Funkschnittstellen aktiviert. Sind etwa GPS oder Bluetooth

aktiv, ohne dass Sie die Schnittstellen eingeschaltet oder bewusst genutzt haben, sollten Sie der Ursache auf den Grund gehen, indem Sie überprüfen, welche Apps gerade aktiv sind (siehe nächster Punkt).
- Nutzen Sie einen Prozessmonitor, um zu überprüfen, welche Anwendungen auf dem Smartphone laufen. Populär sind etwa der Advanced Task Killer (Android) und der SysStats Monitor (iOS, kostenpflichtig). Symbian hat einen integrierten Task Manager, kostenpflichtige Apps wie der "Best TaskMan" sollen aber zusätzliche Informationen bieten.
- In logischer Verlängerung des erstgenannten Arguments, wonach Sie nur Apps installieren sollten, die Sie tatsächlich benötigen: Löschen Sie Apps, die Sie nicht mehr benutzen.

2.5.2 Exkurs: App-Berechtigungen bei Android

Dieser Exkurs bezieht sich nur auf das Betriebssystem Android von Google für Mobiltelefone. Grund hierfür ist, dass der Nutzer bei anderen Systemen, wie Apples iOS oder Windows, die einzelnen Berechtigungen der Apps nicht bestätigen beziehungsweise abwählen kann.

2.5.2.1 Wirkungsweise des Android-Schutzkonzeptes

Applikationen (Apps) für das Betriebssystem Android laufen in einer geschützten, abgeschlossenen Umgebung, einer sogenannten Sandbox. Diese Sandbox bietet zum einen Schutz nach innen, dadurch sind Ihre Benutzerdaten der App vor einem Fremdzugriff geschützt. Zum anderen enthält das Prinzip einen Schutz nach außen. Dieser verhindert, dass die App auf andere Benutzerdaten oder Systemdienste zugreifen kann. Für bestimmte Funktionalitäten wie Datenaustausch und Kommunikation wird die Sandbox mit Hilfe von Berechtigungen (auch Permissions genannt) nach außen hin geöffnet.

2.5.2.2 Berechtigungen

Android kennt etwa 160 verschiedene Berechtigungen, die von Google in Gruppen und Sicherheitsstufen eingeteilt werden. Die Gruppen dienen zur Sortierung der Berechtigungen, sie sagen nichts über die Sicherheit aus. Gruppen sind zum Beispiel:

- **Kostenpflichtige Dienste**
  Ermöglichen Anwendungen die Ausführung eventuell kostenpflichtiger Aktionen.
- **Ihre Nachrichten**
  Lesen und schreiben von SMS, E-Mails und anderen Nachrichten.
- **Ihre persönlichen Informationen**
  Direkter Zugriff auf die Kontakte und den Kalender Ihres Telefons.

Wichtig sind die Sicherheitsstufen, da sie eine Aussage über die Kritikalität der Berechtigung treffen. Folgende vier Stufen unterscheidet Google: 1. normal; 2. dangerous; 3. signature; 4. signatureOrSystem

Für Sie sind **"normal"** und **"dangerous"** relevant, da die zugehörigen Berechtigungen bei der Installation einer App bestätigt werden müssen. Von den in Android definierten Berechtigungen haben 60 die Sicherheitsstufe "dangerous".

Bei der Sicherheitsstufe "dangerous" ist es potenziell möglich, dass mit der jeweiligen Berechtigung eine **missbräuchliche Verwendung** der entsprechenden Funktion durchgeführt wird. Internet-Kriminelle *könnten* somit Ihr Gerät kompromittieren und beispielsweise private Daten ausspionieren.

Im Folgenden sehen Sie zwei Beispiele für Berechtigungen (Quelle: Texte von Android übernommen):

Beispiel: Sicherheitsstufe: dangerous

Berechtigung:	Telefonnummern direkt anrufen.
Beschreibung:	Ermöglicht den Anwendungen, Rufnummern ohne Ihr Eingreifen zu wählen. Schädliche Anwendungen können für unerwartete Anrufe auf Ihrer Telefonrechnung verantwortlich sein. Das Wählen von Notrufnummern ist allerdings nicht möglich.
Gruppe:	Kostenpflichtige Dienste

Beispiel: Sicherheitsstufe: normal

Berechtigung:	Netzwerkstatus anzeigen
Beschreibung:	Ermöglicht einer App, den Status aller Netzwerke anzuzeigen.
Gruppe:	Netzkommunikation

Auswahl kritischer Berechtigungen

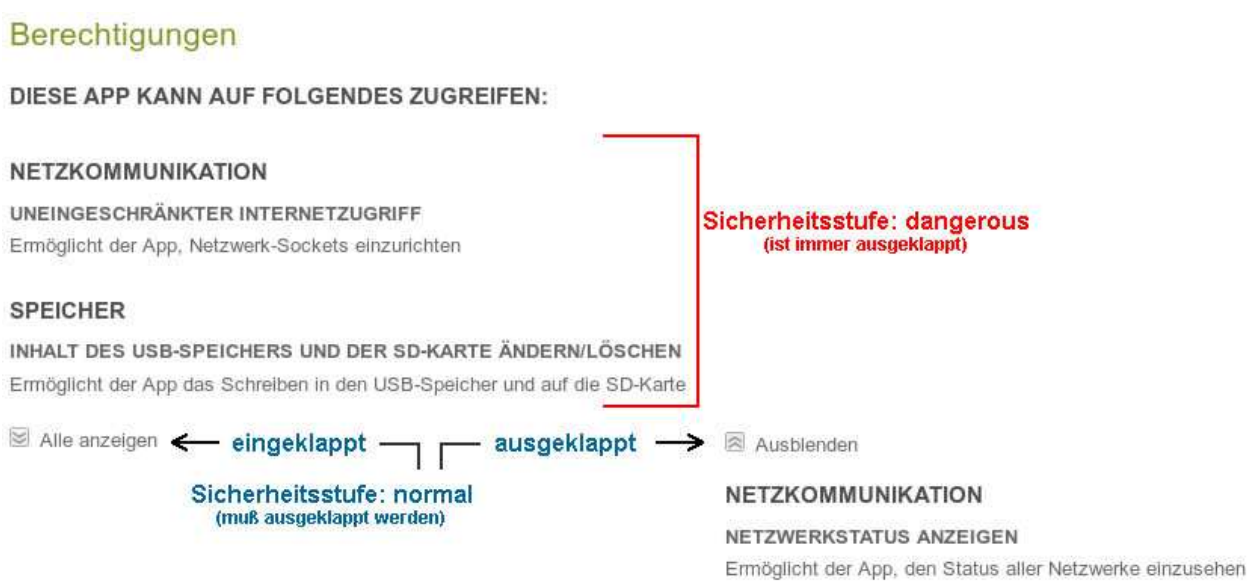
(Quelle: Originalbeschreibungen von Android)

Die folgenden Beispiele zeigen die unterschiedlichen Bereiche, in denen die Apps kritische Berechtigungen fordern können und welche Risiken daraus entstehen.

- **Kostenpflichtige Dienste**
  - *Kurznachrichten senden:*
    Ermöglicht der App das Senden von SMS. Bei schädlichen Anwendungen können Kosten entstehen, wenn diese Nachrichten ohne Ihre Zustimmung versenden.
- **Ihre persönlichen Informationen**
  - *Kontaktdaten lesen:*
    Ermöglicht einer App, alle auf Ihrem Telefon gespeicherten Kontaktdaten (Adressen) zu lesen. Schädliche Apps können so Ihre Daten an andere Personen senden.
  - *In sozialem Stream lesen.*
    Diese Berechtigung ermöglicht der App, auf soziale Updates von Ihnen und Ihren Freunden zuzugreifen und diese zu synchronisieren. Schädliche Apps können mithilfe dieser Berechtigung private Kommunikationen zwischen Ihnen und Ihren Freunden in sozialen Netzwerken lesen.
  - *Kalendertermine sowie vertrauliche Informationen lesen.*
    Ermöglicht einer App das Lesen aller Kalendertermine, die auf Ihrem Telefon gespeichert sind, einschließlich der Termine von Freunden oder Kollegen. Schädliche Apps mit dieser Berechtigung können aus diesen Kalendern ohne das Wissen der Eigentümer persönliche Informationen extrahieren.
  - *Genauer (GPS-) Standort*
    Zugriff auf genaue Standortquellen wie GPS auf dem Telefon (falls verfügbar). Schädliche Apps können damit bestimmen, wo Sie sich befinden und Ihren Akku zusätzlich belasten.
- **Netzkommunikation**
  - *Uneingeschränkter Internetzugriff*
    Ermöglicht einer App, Netzwerk-Sockets einzurichten.
- **Hardware-Steuerelemente**
  - *Bilder und Videos aufnehmen.*
    Ermöglicht der App, Fotos und Videos mit der Kamera aufzunehmen. So kann die App jederzeit Bilder aus dem Sichtfeld der Kamera erfassen.

2.5.2.3 App-Installation

In den verschiedenen App-Stores werden die von einer App benötigten Berechtigungen mit Beschreibung nach Gruppen sortiert aufgelistet. Die Berechtigungen mit der Sicherheitsstufe "dangerous" *werden Ihnen vollständig angezeigt*, während Sie Berechtigungen der Sicherheitsstufe "normal" durch einen Klick auf "Alle anzeigen" *zusätzlich öffnen müssen*. Auch bei Installation der App werden alle "dangerous"-Berechtigungen aufgelistet, die "normal"-Berechtigungen müssen Sie zusätzlich aufklappen.
Wenn Sie eine neue App installieren, müssen Sie die von der App beantragten Berechtigungen bestätigen. Dabei gilt "Alle-oder-keine". Eine differenzierte Genehmigung der App-Berechtigungen ist nicht möglich. Dies führt häufig dazu, dass die beantragten Berechtigungen bestätigt werden, ohne dass die möglichen Gefährdungen bekannt sind.



2.5.2.4 Sicherheitsempfehlungen

Es gelten dieselben Sicherheitsempfehlungen wie für Apps anderer Betriebssysteme. Allerdings gibt es mehr Malware und potenziell unerwünschte Programe (PUP) für Android und auch mehr unseriöse Quellen, Apps zu beziehen als für andere mobile Betriebssysteme. Zudem lassen sich einzelne Berechtigungen nicht abwählen, ohne damit die gesamte Installation abzubrechen. Noch ein Hinweis zu dem Bewertungssystem, auf das Google als "Sicherheitsempfehlung" setzt:

- **Bewertungssysteme:**
  Google setzt stark auf das Bewertungssystem als "Sicherheitsempfehlung": Je mehr Nutzer eine App verwenden und diese positiv bewerten, umso größer soll die Wahrscheinlichkeit sein, dass die App seriös ist, beziehungsweise schädliche Inhalte entdeckt werden.
  Für die Bewertung der Sicherheit einer App ist dieses Kriterium natürlich unbrauchbar. Allerdings kann es in Kombination mit den anderen Kriterien zumindest als Indikator für die Seriosität einer App dienen. Dem BSI ist aber zum Beispiel eine App bekannt, die als Antiviren-Schutz für ein paar Euro verkauft wurde und gute Beurteilungen von Anwendern erhielt. Sie war aber vollkommen wirkungslos.

2.6 Update- und Patch-Management

Patchen, damit Computer, Handy & Co. sicher bleiben.

Ob Betriebssysteme für PC und Laptop, Mediaplayer für das Abspielen von Audio- und Videodateien, Software für Handys oder auch das Virenschutzprogramm – sie alle bieten nur dann sicheren Schutz vor Computerschädlingen, wenn sie auf aktuellem Stand sind.

"Patch", der englische Ausdruck für "Flicken", heißt das Zauberwort:
Dahinter verbergen sich kleinere oder größere Softwarepakete, mit denen die Hersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Unter Sicherheitslücken versteht man dabei Schwachstellen in Software, die es Angreifern beispielsweise ermöglichen, bösartige Programme einzuschleusen und die Kontrolle über fremde Systeme zu übernehmen.
Da viele Nutzer heutzutage zahlreiche verschiedene Softwareprodukte einsetzen, wird es immer schwieriger, den Überblick zu bewahren.
Bei manchen Programmen, etwa Betriebssystemen wie Mac OS X und Windows, erleichtern automatische Update-Services die Aktualisierungsarbeit.
Bei vielen Anwendungen, zum Beispiel dem Virenschutz, ist dies auch schon längst Standard. Vielfach ist es aber der Verantwortung der einzelnen Nutzer überlassen, neue Entwicklungen zu verfolgen und die Software durch das Herunterladen und Installieren von Patches vor Viren, Würmern und sonstigen Angriffen zu sichern – zumindest solange, bis der nächste Computerbösewicht eine vom Hersteller bisher übersehene Lücke findet.

Mit unserem Leitfaden wollen wir Sie dabei unterstützen, ohne allzu großen Aufwand ein System in Ihr Patch-Management zu bringen und sich damit vor bösen Überraschungen zu schützen.

2.6.1 Patch-Management

Leitfaden für sicheres Patch-Management

Beachten Sie die folgenden Maßnahmen, damit Computer, Handy & Co. immer auf dem aktuellen Stand sind und bleiben.

- **Verschaffen Sie sich einen Überblick über die wichtigsten von Ihnen eingesetzten Programme!**
  Dazu zählen neben dem Betriebssystem und dem Browser auch Office-Pakete, Medienplayer, Dienstprogramme von Providern oder das Virenschutzprogramm. Das gilt nicht nur für den PC, sondern auch für die auf dem Laptop, dem PDA oder dem Handy installierten Programme.
- **Prüfen Sie, ob bzw. zu welchen Produkten Sie automatische Update-Services erhalten!**
  Wenn Sie nicht ohnehin wissen, von wem Sie regelmäßig automatisch Updates erhalten, dann nehmen Sie sich kurz Zeit und sehen Sie in Ihrem Softwarevertrag oder in der Online-Hilfe beziehungsweise in den Einstellungen Ihrer Software nach. In der Regel hat man mit der Software einen Anspruch auf ein Jahr technische Unterstützung (Support) und Aktualisierungen bzw. Patches erworben.
- **Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken!**
  Die große Zahl unerwünschter Werbe–Popups, mit denen man als Internetnutzer konfrontiert wird, kann dazu führen, dass man jedes Popup einfach weg klickt. Machen Sie es sich zur Gewohnheit, eine kurze Kontrollsekunde einzulegen und prüfen Sie, ob es sich dabei nicht vielleicht doch um einen wichtigen Warnhinweis handelt.
- **Erstellen Sie eine Übersicht darüber, für welche Programme Sie eigenständig auf Updates achten müssen!**
  Falls Sie feststellen, dass Ihnen für eines oder mehrere zentrale Programme kein automatischer Update-Service zur Verfügung steht, lohnt sich das Anlegen einer Liste. So wissen Sie, welche Produktinfos für Sie von Bedeutung sind.
- **Informieren Sie sich regelmäßig über Updates – etwa durch Newsletter oder Branchenplattformen!**
  Das Bürger-CERT des BSI bietet ein Newsletter-Service an, der Sie über wesentliche Neuerungen informiert. So sind Sie über aktuelle Updates immer auf dem neuesten Stand. Aber auch einzelne Softwareproduzenten oder Brancheninformationsdienste wie www.heise.de oder www.golem.de stellen Warndienste ("Alert Services") per E-Mail und Newsticker zur Verfügung.
- **Laden Sie Patches rasch herunter und installieren Sie sie!**
  Computerbösewichte wissen, dass zumeist schon bald nachdem eine Sicherheitslücke bekannt wird Patches zur Verfügung stehen. Daher versuchen Sie, die Schwachstellen gleich in den ersten Tagen auszunutzen, indem sie Schädlinge wie Viren und Würmer programmieren und in den Umlauf bringen. Nur so können sie soviel Schaden wie möglich verursachen – oder auch maximalen Profit machen. Daher sollten Sie darauf achten, Patches so rasch wie möglich herunter zu laden und zu installieren!
- **ACHTUNG: Lassen Sie sich durch gefälschte Updates nicht aufs Glatteis führen!**
  Leider wird die Bereitschaft zum Patch-Management durch die Programmierer von Computerschädlingen immer wieder für Ihre Zwecke missbraucht: So werden etwa Warn-E-Mails gefälscht und irreführende Popups auf fremde Computer geschmuggelt. Als Richtschnur sollten Sie Updates nur dann installieren, wenn der Hinweis darauf in der Ihnen vertrauten Form erfolgte. Wenn Ihnen E-Mail-Nachrichten mit Aktualisierungshinweisen verdächtig erscheinen, dann folgen Sie den darin enthaltenen Links nicht, sondern informieren Sie sich in Newstickern und tippen Sie die entsprechenden Webadressen manuell ein. Grundsätzlich sollten Sie keine Mailanhänge mit angeblichen Aktualisierungen bzw. Patches öffnen, denn seriöse Firmen verschicken solche Daten nicht per E-Mail.
- **Achten Sie auf Mitteilungen, die das Auslaufen des Supports für Produkte ankündigen!**
  Softwareanbieter bieten Aktualisierungen für einzelne Produkte oftmals nur für einen gewissen Zeitraum an. Beispiel dafür ist etwa die Beendigung des Supports für Windows 98 und für Windows XP durch Microsoft. Auch darüber können Sie sich durch regelmäßigen Besuch der Anbieter-Webseiten oder in Branchendiensten informieren.
- **Installieren Sie, wenn erforderlich, Upgrades für neue Programmversionen!**
  Wenn Hersteller umfassende Änderungen an Ihren Programmen vornehmen, dann erhalten diese Aktualisierungspakete oft eine neue Versionsbezeichnung. Das Programm x in der Version 1.2 wird also beispielsweise durch die Installation eines Upgrades zur Version 1.3. Zumeist sind in solchen Upgrades auch sicherheitsrelevante Änderungen enthalten.

2.6.2 Patch-Management

2.6.2.1 Beispiel "Microsoft Update"

Anhand von "Microsoft Update" lässt sich beispielhaft darstellen, wie Patch-Management für Privatpersonen funktioniert. Nähere Informationen dazu finden Sie auch auf den Webseiten von Microsoft. Hier haben wir für Sie die wichtigsten Punkte zusammen gefasst.

2.6.2.2 Was ist Microsoft Update?

Microsoft bezeichnet damit einen Teil seiner Webseite, auf dem die neuesten Updates für all seine Programme – vom Betriebssystem Windows über den Browser Internet Explorer bis hin zu Outlook oder dem Movie Maker – bereit gestellt werden.

2.6.2.3 Wie stellen Sie fest, ob Sie Aktualisierungsbedarf haben?

Ihren Update-Service finden Sie je nach Betriebssystemversion unter Start > (Einstellungen) > Systemsteuerung. Bei manchen Betriebssystemen sehen Sie an dieser Stelle schon den Hinweis "siehe auch Windows Update" mit einem entsprechenden Link. Wenn kein Hinweis auftaucht, so gehen Sie weiter zu > Software > neue Programme installieren > Windows Update". Ihr Computer wird danach automatisch auf veraltete Software überprüft, die entsprechenden Updates werden Ihnen zum Download angeboten. Nach Updates für Microsoft-Office-Programme wie Word, Excel oder PowerPoint können Sie übrigens unter der Funktion Office Update suchen.

2.6.2.5 Wie installieren Sie die Updates?

Markieren Sie die Kästchen neben den Updates, die in der Liste angeführt werden und klicken Sie auf "Updates installieren".

Wie automatisieren Sie den Update Service?

Microsoft beschreibt auf seiner Webseite "Microsoft Safety & Security Center" die Möglichkeiten, wie Sie die automatische Ausführung von Updates aktivieren und Updates ausführen können.

Was müssen Sie selbst noch tun, wenn Sie automatische Updates beziehen?

Sie können selbst einstellen, in welchem Umfang Sie am Update-Vorgang beteiligt sein wollen. Je nachdem startet Ihr PC nach dem Download neuer Updates sofort mit dem Installationsvorgang oder informiert Sie mit einer Info bzw. einem Warnhinweis. In diesem Fall können Sie dann selbst aussuchen und anklicken, was installiert werden soll.

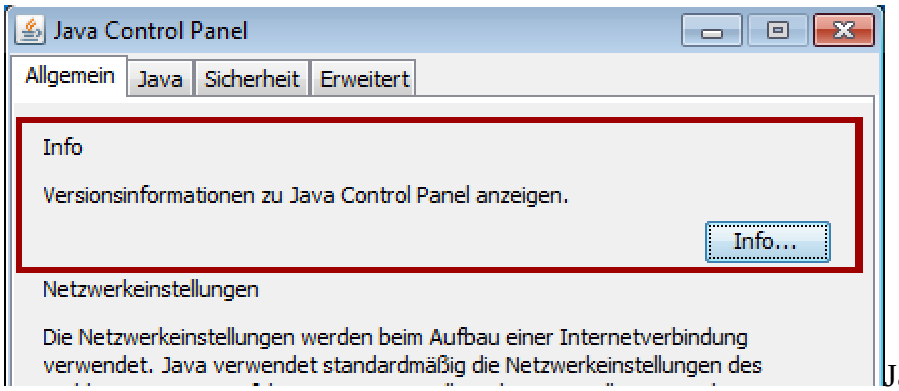
2.6.2.6 Was ist der Microsoft Patch-Day?

An jedem zweiten Dienstag im Monat (durch die Zeitverschiebung zwischen den USA und Europa bei uns meist spät abends) veröffentlicht Microsoft jüngste Aktualisierungen. Wenn dringender Handlungsbedarf besteht, wird dieser Rhythmus allerdings auch durchbrochen.

2.6.3 Update von Java

2.6.3.1 Wie stellen Sie fest, ob Sie Aktualisierungsbedarf haben?

Ob die installierte Java-Version auf Ihrem Computer aktuell ist, erfahren Sie über einen Test auf der Java Webseite oder manuell über das Java Control Panel.

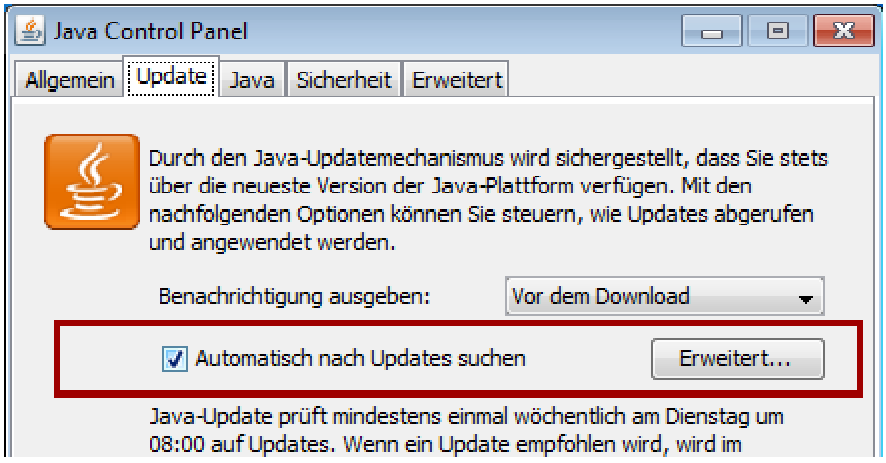


Java Control Panel > Reiter Allgemein

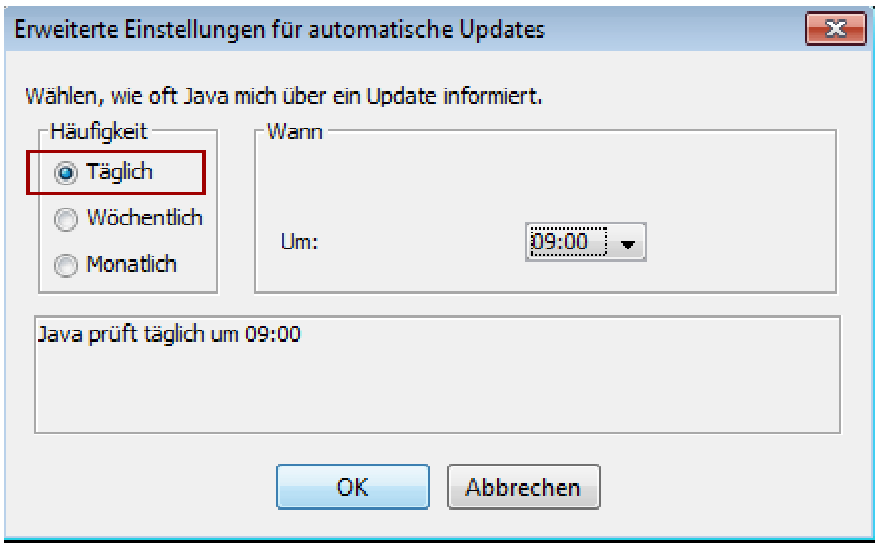
Nach dem Klick auf die Schaltfläche "Info" wird die derzeitige Java Version angezeigt.

2.6.3.2 Wie installieren Sie ein Update?

Ist Java bereits auf Ihrem Computer installiert, sollten Sie den Updatemechanismus von Java so einstellen, dass ***täglich*** nach Aktualisierungen gesucht und diese ggf. automatisch installiert werden. Der Updatemechanismus erreichen Sie über den Reiter "Update" im Java Control Panel.



Nach dem Klick auf die Schaltfläche "Erweitert" gelangen Sie zu den Updateeinstellungen.



Das Update bzw. die Suche nach verfügbaren Updates können Sie jederzeit durch Betätigung der Schaltfläche "Jetzt updaten" manuell starten.

Hilfestellung zu diesem Thema erhalten Sie unter
http://www.java.com/de/download/help/java_update.xml

Warum finde ich den Reiter "Update" nicht?

Java-Autoupdate ist vor Java 8 für 64-Bit-Versionen von Java nicht verfügbar. Für Versionen vor Java 8 ist die Registerkarte "Update" im Java Control Panel nicht verfügbar.

Ab Java 8 Update 20 können Benutzer in der Registerkarte "Update" im Java Control Panel die im System installierten 64-Bit-JREs (zusätzlich zu 32-Bit-Versionen) automatisch updaten. [Quelle: Java Webseite]

2.6.3.5 Veraltete Versionen von Java deinstallieren

Auf folgender Seite wird erklärt, wie Sie ältere Versionen von Java manuell deinstallieren können:
http://www.java.com/de/download/help/uninstall_java.xml

Mit Hilfe des Java Uninstall Tools können Sie veraltete Versionen von Java ebenfalls deinstallieren.

Das Tool ist in Form eines Applets und nur für Windows-System unter folgendem Link verfügbar:
http://www.java.com/en/download/uninstallapplet.jsp

2.7 Fragen & Antworten zu Open Source Software

2.7.0 Schnell zum Abschnitt

2.7.1 Was heißt Open Source Software (OSS)?

Open Source Software unterscheidet sich von **herstellergebundener** (proprietärer) Software darin grundlegend, dass der **Quellcode** – das ist in etwa das was bei einem Haus der Bauplan ist – frei verfügbar ist. Das bedeutet, dass der Anwender das Programm unabhängig von seinen Autoren in der Regel beliebig verändern, weitergeben und erkannte Schwachstellen oder Fehler veröffentlichen darf.

Weil der Quellcode jedem offen zugänglich ist, wird solche Software Open Source Software genannt. Alternativ wird auch der Begriff **Freie Software** verwendet, der sich auf die Freiheiten des Anwenders bezieht, das Programm einzusetzen, zu verändern und weiterzugeben. Im Vergleich dazu kann der

Nutzer ein proprietäres Programm weder prüfen noch verändern. Er kann es noch nicht einmal lesen oder verstehen.

2.7.2 Wann ist Software Open Source Software?

Es gilt einige Kriterien zu erfüllen, damit sich eine Software "Open Source Software" nennen darf.

- Das Programm darf ohne Beschränkungen eingesetzt werden.
- Es ist erlaubt zu studieren, wie das Programm arbeitet und es an die eigenen Bedürfnisse anzupassen. Dazu muss der Quelltext der Software in einer für den Menschen lesbaren und verständlichen Form vorliegen.
- Kopien des Programms dürfen weitergegeben werden, so dass auch andere es nutzen können.
- Das Programm darf verbessert und die Verbesserungen dürfen weitergegeben werden.

2.7.3 Warum gibt es Open Source Software?

Die Philosophie von Open Source Software geht zurück auf den Grundgedanken des **freien Austauschs** von Wissen und Gedanken. Software kann, wie auch Ideen, jedem frei zur Verfügung gestellt werden – ohne Verluste. Wird Software weitergeben, entwickelt sie sich wie in einem **evolutionären Prozess**.

Ein Beispiel:
Nehmen wir an, Sie brauchen eine Software, die es aber nicht zu kaufen gibt. Sie müssen also selbst eine Software entwickeln, testen und haben allen Aufwand, den so etwas mit sich bringt. Eigentlich würde es Ihnen aber nichts ausmachen, wenn auch andere das Programm benutzen würden. Im Gegenteil, Sie würden sogar von der Erfahrung und von der Beteiligung weiterer Nutzer **profitieren**. Grund genug, Ihr Software-Projekt zu beginnen und es sobald wie möglich als Open Source-Projekt zu veröffentlichen. Sie geben dann Ihr Programm für die Verwendung frei und profitieren im Austausch von der zusätzlichen **Kapazität** und **Expertise** der anderen Entwickler und Anwender. Dabei kann es Ihnen egal sein, ob nur ein kleiner Teil oder alle Anwender zur weiteren Entwicklung beitragen.

2.7.4 Ist Open Source Software genauso sicher wie proprietäre Angebote?

Ja. Weil viele Programmierer in aller Welt – man nennt sie "**Community**" oder Entwickler-Gemeinschaft – die Möglichkeit haben, sich den Quelltext der Software anzusehen. So können sie mögliche Probleme rasch erkennen und gegebenenfalls sofort beheben. Denn: Viele Augen sehen viel! Die Entwickler sind normalerweise namentlich bekannt. Keiner von ihnen würde sich gerne nachsagen lassen, er habe **schädliche Software** programmiert.

Bei Open Source Software gibt es zudem immer die Möglichkeit, **Warnmeldungen** ins Internet zu stellen, wenn Sicherheitslücken gefunden wurden. So existiert praktisch eine Art **Frühwarnsystem**, das dem Nutzer die Möglichkeit gibt sich abzusichern.

Ein weiterer Sicherheitsaspekt ist, dass Open Source Software bislang selten von Viren befallen wird. Das liegt natürlich zum einen daran, dass sie noch nicht so stark verbreitet ist, wie proprietäre Software, aber auch daran, dass sicheres Programmieren und **Sicherheitsfunktionen** im Bereich der Open Source Software traditionell einen hohen Stellenwert haben.

2.7.4.1 Sicherheitstipp:

Bei Open Source Software gilt jedoch das Gleiche wie bei proprietärer Software: Laden Sie nichts einfach aus dem Internet auf Ihre Festplatte. Anbieter stellen in der Regel die Möglichkeit zur Überprüfung der Echtheit des Programmes zur Verfügung. Diese ist in der Installationsanleitung zu finden. Erst nach erfolgreicher Prüfung sollte man die Software installieren. Einfacher – und für den unerfahrenen Nutzer sicherer – ist es, die Software nach Möglichkeit aus den Repositories der eingesetzten Distribution (z. B. Ubuntu GNU/Linux) zu beziehen, welche mit Prüfsummen und Signaturen versehen sind, die von der eingesetzten Distribution automatisch geprüft werden. Im Falle von Ubuntu kann z. B. auf das Repository direkt über das in die Oberfläche des Betriebssystems integrierte "Software-Center" zugegriffen werden.

2.7.5 Wer ist bei Problemen mit Open Source Software zuständig?

Ist ja alles schön und gut, könnten Sie denken, aber was, wenn ich einmal Probleme mit Freier Software habe. Fühlt sich denn da überhaupt jemand **verantwortlich**, wenn eigentlich alle mit entwickeln? Keine Sorge, es gibt sogar Untersuchungen, die beweisen, dass die **Unterstützung** für Open Source Software

oft besser ist als die für herstellergebundene Angebote. Anwender erhalten offizielle Unterstützung, wenn Sie das zusammengestellte Software-Paket eines Open Source-Distributors (z. B. Ubuntu, SuSE/Novell, Mandrake, ...) über den Handel kaufen. Experten können allerdings auch **komplexe Probleme** mit Hilfe der Community schnell lösen. Bei proprietärer Software ist es nötig, erst das Entwicklungsteam des Herstellers zu kontaktieren.

2.7.6 Beispiele für Open Source Software

Inzwischen ist Open Source Software eine **anerkannte Alternative** zu proprietären Angeboten. Besonders die Europäische Union und zahlreiche öffentliche Verwaltungen unternehmen erhebliche Anstrengungen, um den Einsatz von Open Source Software zu fördern. Auch große Konzerne wie etwa Google, IBM, Hewlett Packard oder Intel sind Förderer von Open Source Software und Entwicklungen. Selbst **prominente Hersteller** proprietärer Software wie Adobe, Apple, Microsoft, Oracle oder SAP haben zahlreiche Berührungspunkte zur Open Source-Bewegung oder bieten ihre Produkte auch für das Betriebssystem GNU/Linux an.

Deshalb gibt es mittlerweile auch viele Programme, die als Open Source Software angeboten werden. Neben Tools für die Programmentwicklung und für die professionelle Betreuung von Servern und Netzwerken gibt es eine Fülle von Anwendungsprogrammen für den **täglichen Einsatz** im Unternehmen oder anderswo.

2.7.6.1 Einige Beispiele:

- GNU/Linux ist ein sehr leistungsfähiges Betriebssystem für eine Vielzahl von Plattformen und ist das Paradebeispiel für ein erfolgreiches Open Source-Projekt. Den Kern hat 1991 der damals 21-jährige Linus Torvalds dazu beigetragen. Seither wird es von einer Vielzahl an Entwicklern aus aller Welt weiterentwickelt. Prominentes Beispiel für den Stellenwert von GNU/Linux ist der Deutsche Bundestag. Im Serverbereich werden dort GNU/Linux und andere Open Source Software eingesetzt.
- LibreOffice.org ist ein freies Office-Programm, das auf GNU/Linux- und auf Microsoft-Betriebssystemen, sowie auf MacOS X und weiteren Betriebssystemen läuft. Es beinhaltet alle notwendigen Funktionen wie Textverarbeitung-, Tabellenkalkulation- und Präsentationsprogramm. Die Bedienung ist ähnlich wie bei anderen Office-Programmen und viele offene Dateiformate, aber auch das proprietäre Microsoft Word Format lassen sich damit bearbeiten.
- Die Internetbrowser Firefox und Chrome sind ebenfalls für viele verschiedene Betriebssysteme verfügbar. Der Quellcode von Firefox stammte ursprünglich von Netscape. Chrome verwendet mit WebKit an zentraler Stelle eine OSS-Komponente, die u. a. auch von dem proprietären Browser Safari eingesetzt wird.
- Der Web-Server Apache zählt neben GNU/Linux zu den erfolgreichsten Open Source-Projekten. Mehr als die Hälfte aller Web-Server arbeiten mit dieser Software.

2.7.7 Und zum Schluss: Ist Open Source Software immer kostenlos?

Fast immer ja, aber genau hier liegen häufig Missverständnisse in Bezug auf Open Source Software. Prinzipiell kann Freie Software zwar auch verkauft werden, wie z. B. einige GNU/Linux-Distributionen, die als DVD gekauft werden können. Aber es müssen auch bei kostenpflichtig erworbener Freier Software die oben angeführten Bedingungen für Freie Software eingehalten werden, so dass der Verkauf Freier Software eher eine Ausnahme ist und der Preis sich oftmals nahe am Selbstkostenpreis bewegt. Möchte der Anwender neben der reinen Software aber noch Dienstleistungen wie Handbücher oder Support in Anspruch nehmen, so muss er die Zusatzleistungen bezahlen. Diese erhält er in Form einer gängigen GNU/Linux-Distribution (das ist eine Zusammenstellung von Softwarepaketen), die unter anderem im Buchhandel erhältlich ist.

Einige Beispiele anderer kostenloser Vertriebsformen sind:

- **Freeware** ist Software, die kostenlos genutzt werden kann. Andere Kriterien für Freeware gibt es nicht.
- **Shareware** kann zunächst kostenfrei installiert und verwendet werden. Später kann der Autor für die Nutzung oder für bestimmte Formen der Nutzung Lizenzkosten verlangen. Der Autor verzichtet lediglich auf die Prüfung oder auf Maßnahmen zur Sicherstellung dieser Lizenzzahlungen. Manchmal steht Anwendern bis zur Bezahlung der Lizenzen – also bis zur Registrierung – nur ein reduzierter Funktionsumfang zur Verfügung.

2.8 Vorabversionen neuer Betriebssysteme

Sie möchten eine Vorabversion eines neuen Betriebssystems testen – dann sollten Sie folgendes beachten.

Sobald die großen Anbieter neue Versionen ihrer Betriebssysteme ankündigen, steigt die Neugier auf die beworbenen neuen Funktionen der Software. Inzwischen ist es üblich, dass Apple, Google oder Microsoft Vorabversionen ihrer Betriebssysteme bereits vor der offiziellen Markteinführung zur Verfügung stellen. Die Versionen heißen dann Golden Master, Technical Preview oder Public Beta.

Wenn Sie eine Vorabversion eines neuen Betriebssystems ausprobieren möchten, sollten Sie unsere Tipps beachten, um eine Gefährdung der Sicherheit Ihres Rechners und insbesondere Ihrer Daten zu vermeiden.

- Seien Sie sich darüber bewusst, dass es sich bei diesen Vorabveröffentlichungen um teilweise noch fehlerbehaftete Versionen der Software handelt. **Setzen Sie sie daher auf gar keinen Fall zur Verarbeitung oder Speicherung Ihrer persönlichen oder geschäftlichen Daten ein.**
- Die Testversionen sind mit **keinerlei Gewährleistungen** seitens der Hersteller verbunden. Verfügbarkeit, Vertraulichkeit und Integrität Ihrer Daten werden in der Regel nicht durchgängig sichergestellt.
- In einigen Fällen ist es dem Hersteller sogar gemäß der von ihm vorgegebenen Bedingungen zur Nutzung von Vorabversionen ausdrücklich gestattet, auf Ihre persönlichen Daten, Ihr vollständiges Nutzungsverhalten bis hin zu Ihren Tastatureingaben über das Netz zuzugreifen oder Telemetriedaten zu verwenden.
- Es ist demnach nicht zu empfehlen, Ihren üblicherweise genutzten Mac-, Windows- oder Chrome-OS-Rechner durch ein System mit einer Vorabversion zu ersetzen. **Idealerweise nutzen Sie für den Test einen separaten Rechner**.
- Nutzen Sie auch nicht die vorhandenen Internetverbindung des Testsystems zum Aufruf von Cloud- und Web-Diensten wie E-Mail, Online-Banking oder Shoppingportalen. Verwenden Sie sowohl lokal als auch im Internet auf Testsystemen nur Testpasswörter, die in keinem Zusammenhang mit den üblicherweise von Ihnen verwendeten Passwörtern stehen.
- Von der Einrichtung einer Parallelinstallation auf einem System, dass auch Ihre normale Arbeitsumgebung starten kann, ist in jedem Fall abzuraten. Vorabversionen von Betriebssystemen können zudem auch die Bootinformationen beeinflussen oder überschreiben.

2.8.1 Bei allen diesen Nachteilen – wofür gibt es dann Testversionen?

Das Vorgehen der Entwickler von neuen Betriebssystemen ist durchaus nachvollziehbar und sinnvoll: Es sollen bereits vor der Markteinführung möglichst viele der noch möglichen vorhandenen Fehler beseitigt werden. Daher müssen diese Nutzungsdaten erfasst und an den Hersteller übertragen werden. Dort werden sie dann zentral ausgewertet. Wenn Sie selbst eine Vorabversionen der Betriebssysteme ausprobieren, werden Sie Teil des weltweit verteilten Testlabors des Herstellers.

Eine elegante Möglichkeit, neue oder andere Betriebssystemvarianten auszuprobieren, stellen virtualisierte Umgebungen dar. Hier ist allerdings vorab zu prüfen, ob dies seitens des Herstellers technisch möglich und lizenzrechtlich gestattet ist.

2.8.2 Fazit

Vorabversionen von neuen Betriebssystemen richten sich an technisch Interessierte, die sich den Randbedingungen, die mit solchen Tests verbunden sind, bewusst sind. Wenn Sie die oben beschriebenen Empfehlungen befolgen, sind Sie auf der sicheren Seite. Steht Ihnen ein Testrechner zur Verfügung, lohnt sich ein Blick auf die kommende Version Ihres Betriebssystem oder auch ein Blick auf alternative Produkte.

So können Sie sich schon vorab mit neuen Funktionen vertraut machen, zu denen oftmals auch Verbesserungen der Sicherheitseigenschaften gehören. Nur Ihre Daten sollten Sie einem neuen Produkt immer erst dann anvertrauen, wenn der Hersteller dessen Funktionsfähigkeit in einer stabilen Version garantiert.