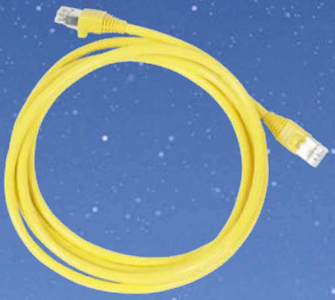
Mit dem Mac sicher ins Internet

Ein Leitfaden für Internetnutzer



macsicherheit.de

Nutzungsbedingungen

Die Empfehlungen, die ich in diesem Dokument dargestellt habe, sind meine private Meinung zu dem Thema und können für den nicht kommerziellen Zweck verwendet werden. Jeder sollte die Empfehlungen vor der Anwendung eindringlich prüfen. Haftung vor aller Art von Schäden, die durch Anwendung der folgenden Empfehlungen entstehen, kann ich nicht übernehmen. Insgesamt gelten die Nutzungsbedingungen wie unter folgenden Link beschrieben:

http://www.macsicherheit.de/index.php/nutzungsbedingungen.html

Das Internet ist grundsätzlich unsicher

Das Internet nimmt in unserer Gesellschaft eine immer größere Rolle ein. Es dient der Informationsgewinnung, der Kommunikation und der freien Meinungsäußerung. Es wird aber auch bei sensiblen Diensten wie Online Banking und Online Shopping eingesetzt. Auch die Kommunikation mit Behörden oder Geschäftspartnern bzw. Kunden findet verstärkt über das Internet statt. Gleichzeitg nimmt die Bedrohung im Internet durch Kriminelle, durch Geheimdienste, selbst befreundeter Staaten, und durch die Datensammelwut von Wirtschaftsunternehmen zu.

Das Internet ist grundsätzlich unsicher. Daher muss jeder Nutzer selber grundlegende Sicherheitsmaßnahmen und Verhaltensweisen erlernen und beachten.

Wissen ist Macht

Das Internet ist kein Buch mit sieben Siegel. Ganz im Gegenteil: es bietet mächtige Werkzeuge, Informationen zu finden und damit eigenes Wissen aufzubauen oder zu vertiefen. Insbesondere Suchmaschinen lassen sich hierfür nutzen. Die wohl bekannteste und in Deutschland am häufigsten genutzte Suchmaschine ist die von Google. Andere Suchmaschinen sind Bing von Microsoft oder Yahoo. Eine weitere Alternative ist DuckDuckGo. Während die großen Suchmaschinenbetreiber versuchen, möglichst viele Daten über ihre Nutzer zu sammeln und Nutzerprofile anlegen, verspricht DuckDuckGo mehr Anonymität. Aber auch bei diesen Betreiber handelt es sich um ein amerikanisches Unternehmen. Diese sind in den letzten Monaten in den Verdacht geraten, mit dem US-Geheimdienst NSA zusammen zu arbeiten und den Spionen Zugriff auf die Nutzerdaten zu gewähren. Eine europäische Alternative ist Startpage bzw. ixquick. Der niederländische Betreiber, der europäische Datenschutzrichtlinien umzusetzen hat, fungiert als eine Art Vermittler. Er nimmt die Suchanfragen entgegen und leitet sie anonymisiert weiter an die großen Suchmaschinen. So kann Google und Co keine Profile erstellen, die Ergebnisse sind aber auch nicht personalisiert. Ähnlich verfährt die Suchmaschine MetaGer der Leibniz Universität Hannover. Disconnect bietet eine Browser-Erweiterung, die Suchanfragen bei verschiedenen Suchmaschinen anonymisiert.

Wer das Internet mit seinen Rechner sicher nutzen und auch keine Gefahr für andere Internetnutzer darstellen möchte, sollte sich umfassend mit dem Thema auseinander setzen. Dazu lassen sich Suchmaschinen wirkungsvoll einsetzen. Zur Hilfe gebe ich in den nächsten Abschnitten jeweils am Ende Suchbegriffe an, die man in die Suchmaschine der Wahl eingeben kann, um weitergehende Informationen zu erhalten. Auch die Seiten wikipedia.de, www.bsi-fuer-buerger.de sowie macsicherheit.de sind sehr hilfreich. Die meisten angegebenen Suchbegriffe sowie weiterführende Informationen werden hier erläutert.

Suchbegriffe: Suchmaschinen, Alternative Suchmaschinen, Google, Bing, Yahoo, DuckDuckGo, Startpage, ixquick, MetaGer, Disconnect, Wikipedia, BSI, BSI für Bürger, Sicherheitstest, Macsicherheit

Den Rechner absichern

Ein am Internet angeschlossener Rechner ist zahlreichen Angriffen ausgesetzt. Z.B. versuchen Internetkriminelle Schadprogramme unbemerkt auf Rechner zu installieren.

Damit haben sie oft vollen Zugriff auf alle Daten und Anwendungen. Sie können nicht nur persönliche Daten auslesen, sondern sie versuchen auch Passwörter, PIN- und TAN-Nummern auszuspähen. Außerdem sind die Kriminellen in der Lage, die Internetanbindung des betroffenen Rechners für weitere kriminelle Handlungen zu nutzen. So versenden sie darüber Spam, E-Mails mit Schadprogrammen im Anhang, um weitere Nutzer anzugreifen oder sie starten Angriffe auf die Verfügbarkeit von Internetportalen, um deren Betreiber zu erpressen. Es liegt also nicht nur im eigenen Interesse, seinen Rechner abzusichern, sondern auch im Interesse der Allgemeinheit, weil ein infizierter Rechner für Internetstraftaten gegen andere missbraucht werden kann. Er wird dann als „Waffe" gegen andere Menschen eingesetzt. Daher sollte mah sich mit der Sicherheit des eigenen Rechners beschäftigen, um sich und andere zu schützen. So macht man es z.B. auch im Straßenverkehr. Auch hier muss man die Verkehrsregeln beachten, um Unfälle zu verhindern. Autofahrer sind für die Verkehrstüchtigkeit ihres Wagens verantwortlich. Folgende grundlegende Maßnahmen sollte man daher umsetzen:

- Man sollte sich eingehend mit der Sicherheit seines Rechners auseinandersetzen.
- Regelmäßig stellen die Hersteller Softwareupdates für Betriebssystem und Anwendungen zur Verfügung. Diese sollten unverzüglich eingespielt werden, da häufig auch Sicherheitslücken geschlossen werden. Um ein Update nicht zu verpassen, sollte man, falls verfügbar, die Auto-Update-Funktion aktivieren.
- Zur Sicherheit des eigenen Rechners trägt auch eine Personal-Firewall bei. In der Regel genügt es, die bereits im Betriebssystem verankerte Firewall zu aktivieren. Zusatzprodukte bieten meist weitergehenden Schutz.
- Ein Virenscanner sollte nicht fehlen, damit Daten nach dem Empfang oder vor der Weitergabe auf Schadprogramme getestet werden können.
- Bei der Nutzung des Internets ist umsichtiges Verhalten dringend angeraten. Nicht jeder Anhang in E-Mails oder jede Webseite bzw. jeder Download ist seriös. Gesundes Misstrauen und z.B. eine Nachfrage beim Absender der E-Mail kann den eigenen Rechner vor Schaden bewahren.
- Es sollten nur sichere Passwörter verwendet werden. Ein sicheres Passwort ist mindestens zehn Zeichen lang und so komplex, dass andere es nicht erraten können. Es beinhaltet gemischt Groß- und Kleinbuchstaben, Ziffern und Zeichen.

Suchbegriffe: Schadprogramme, Viren, Trojaner, Würmer, Bots, Botnetze, Virenscanner, Personal Firewall, Sicherheitslücken, Sicherheitsupdates, Auto-Update, Sicherer PC, Spam, DDoS

Einen sicheren Provider auswählen

Bevor man das Internet nutzen kann, wird ein Internetservice Provider benötigt. Dieser stellt den Anschluss mit der vertraglich vereinbarten Bandbreite zur Verfügung. Daran angeschlossen wird meist ein Router, mit den man seine Rechner über Kabel oder WLAN verbindet. Häufig wird der Router vom Provider bereitgestellt und konfiguriert. In diesem Fall sollte man darauf achten (und ggf. beim Support nachfragen), dass der Provider eine sichere Einstellung vornimmt und Sicherheitsupdates des Routers schnellstmöglich einspielt. Die WLAN-Einstellungen übernimmt der Kunde in der Regel selber. Hierbei sollte man die sichere WLAN-Verschlüsselung „WPA2" aktivieren und ein gutes

WLAN-Kennwort (komplex und mindestens 20 Zeichen lang) auswählen.
Ein guter Provider bietet seinen Kunden aus meiner Sicht ein gegen Spam und Schadprogramme geschütztes E-Mail-Postfach an. Des Weiteren informiert er betroffene Kunden, wenn er Kenntnis erlangt, dass Kundenrechner mit Schadprogrammen infiziert sind oder andere Sicherheitsprobleme vorliegen. Natürlich schützt er seine eigene Systeme, insbesondere jene, die die Kundendaten enthalten. Auch beim Thema Datenschutz verhält sich der Provider vorbildlich. Hierzu sollte man sich die Zeit nehmen und die Datenschutzerklärung sorgfältig lesen. Überall dort, wo eine verschlüsselte Verbindung möglich ist, setzt ein guter Provider diese mit der höchsten Sicherheit ein, ohne dass den Kunden große Aufwände oder Funktionseinbußen entstehen.
Leider geben sich viele Provider nicht immer transparent, wenn es um die Offenlegung ihrer Sicherheitsdienstleistungen geht. Hier hilft dann häufig nur, beim Support nachzufragen oder in den Untiefen des Webportals nachzuforschen. Im Zweifelsfall wählt man einen anderen Provider aus.

Suchbegriffe: Internetservice Provider, WLAN, WPA2, Verschlüsselung, DSL-Router, Kabel-Router, E-Mail-Postfach, Datenschutzerklärung, Provider Sicherheitsdienstleistungen

Sicher Surfen

Einer der wichtigsten Dienste im Internet ist das World Wide Web: das „Surfen“ bzw. die Informationsbeschaffung mittels Webbrowser. Leider kann man auch dabei angegriffen werden. Das bloße Aufrufen einer Webseite mit einem verwundbaren Webbrowser kann dazu führen, dass der eigene Rechner mit einem Schadprogramm infiziert wird. Die Kriminellen nutzen hier zum einen Schwachstellen des Browsers aus und zum anderen manipulieren sie sogar seriöse Webseiten, deren Betreiber Sicherheitsprobleme übersehen haben. Dort injizieren sie zumeist einen Programmcode, der die Installation des Schadprogramms auf den betroffenen Rechner bewirkt. Dagegen kann man sich schützen, indem man die Angriffsfläche verringert.

- Keine unseriösen Webseiten besuchen und dort heruntergeladene Daten ausführen, da hier die Gefährdung größer ist als bei seriösen Webseiten.
- Regelmäßig die Updates des Webbrowsers installieren, sobald sie der Hersteller zur Verfügung stellt.
- Nur wirklich notwendige Plug-Ins (das sind Erweiterung des Funktionsumfangs, die zusätzlich installiert werden müssen) installieren, da diese auch Schwachstellen enthalten können und daher mittels eigener Updates zusätzlich gepflegt werden müssen.
- Viele Angriffe erfolgen über Flash-Inhalte (bewegte Bilder, Videos auf Webseiten). Daher sollten nicht benötigte Flash-Inhalte erst gar nicht geladen werden (ist auch häufig nur Werbung). Dazu bieten gängige Webbrowser eigene Funktionen an oder es existieren Plug-Ins, die man installieren kann. Sogenannte Flash-Blocker blockieren Flash-Inhalte und zeigen stattdessen nur ein spezifisches Symbol an. Klickt man jedoch bewusst darauf, wird der Flash-Inhalt geladen und angezeigt.
- Auf Java-Inhalte kann man meistens ganz verzichten. Entsprechende Plug-Ins können deaktiviert werden.
- Wer auf Nummer sicher gehen will, der deaktiviert Java-Script. Das ist aber mit vielen Einschränkungen verbunden. Alternativ installiert man sich Plug-Ins wie z.B. NoScript. Hiermit kann man gezielt Java-Script auf vertrauenswürdigen Webseiten freischalten und ansonsten generell blockieren.
- Viele Browser weisen Nutzer auf bekannte schädliche Webseiten hin. Diese Funktion sollte nicht deaktiviert werden.

- Passwörter oder andere vertrauenswürdige Daten sollten nur auf Webseiten eingegeben werden, die eine Verschlüsselung anbieten. Das erkennt man häufig an den angezeigten Schlöß-Symbol oder der Bezeichnung https in der Adressleiste des Browsers.

Suchbegriffe: Webbrowser, Firefox, Internet Explorer, Safari, Chrome, Adressleiste, Plug-In, Flash, Flash-Blocker, Java, Java Script, NoScript, Safebrowsing, Smart Screen, SSL, https

Sichere E-Mails

Auch der E-Mail-Dienst wird häufig benutzt. Neben Spam-Mails findet man häufig auch sogenannte Phishing-Mails im Postfach. Kriminelle versuchen hier ihre Opfer auf präparierte Webseiten zu locken, die zu einer Infektion des Rechners führen oder wo man unter einem Vorwand vertrauliche Daten eingeben soll. Auf derartige Betrügereien darf man auf keinen Fall hereinfallen! Auch Schadprogramme befinden sich häufig in E-Mails. Daher sollte man beim Öffnen von Anhängen sehr vorsichtig sein. Ist die Quelle unbekannt, ist grundsätzlich davon Abstand zu nehmen. Aber auch bei bekannter Quelle ist es sinnvoll, beim Absender nachzufragen. Das gilt insbesondere dann, wenn man mit der E-Mail nicht rechnet oder sie ungewöhnlich aussieht.

Die Internetservice Provider bieten für die Mailpostfächer ihrer Kunden häufig Viren- und Spamschutz an. Aus meiner Sicht sollte man hierauf nicht verzichten, selbst wenn man noch zusätzlich eigene Maßnahmen getroffen hat. Nachteil ist, dass die E-Mails in den Postfächern umverschlüsselt vorliegen müssen. Daher sollten besonders schützenswerte E-Mails oder Anhänge auf dem eigenen Rechner verschlüsselt werden. Hierzu bieten sich Programme wie z.B. GnuPG an. Der Provider selber sollte in jedem Fall für eine Transportverschlüsselung sorgen und die Postfächer seiner Kunden bestmöglich absichern.

Suchbegriffe: Phishing, Kurz-URLs, E-Mail-Postfächer, E-Mail-Verschlüsselung, GnuPG, GPG, Gpg4Win, pretty good privacy, E-Mail made in Germany, De-Mail, DANE, Posteo

Private Daten sind privat

Wer Daten im Internet veröffentlicht, verliert die Kontrolle über diese Daten. Internetfirmen sammeln Daten und verknüpfen sie miteinander, um Nutzerprofile zu erstellen. Diese Profile werden für personalisierte Werbung verwendet, ein Geschäftsmodell, das häufig im Internet anzutreffen ist. Dagegen hilft nur, genau abzuwägen, welche Daten z.B. in Sozialen Netzen oder in Online-Foren preisgegeben werden. Auch die Datenschutzerklärungen und die Nutzungsbedingungen sollten studiert werden, um entscheiden zu können, ob die Nutzung des ausgewählten Dienstes in Frage kommt oder nicht.

Beim Besuch kommerzieller Nachrichtenportale werden Daten oft zu Werbezwecken gesammelt. Hier kann man sich mit Werbe- und Trackingblocker schützen. Geläufige Blocker sind AdBlock und Ghostery aber auch Disconnect bietet eine Browser-Erweiterung an, mit der Tracking geblockt werden kann. Aktuelle Versionen von Firefox verwendet die Blockliste von Disconnect, um im Privaten Modus Tracking-Dienste zu filtern. Cookies sollten nicht für Dritte freigegeben und automatisch nach Schließen des Browsers gelöscht werden. Manche Webbrowser verfügen über einen Privaten Modus, den man bei Bedarf aktivieren kann. Der Zugriff von Webseiten auf den eigenen Aufenthaltsort (Geolokalisierung) sollte ebenfalls verhindert werden.

Europäische Cloud-Dienste sind aus Datenschutzgründen vorzuziehen. Zumindest sollten

die Daten zuvor auf dem Client verschlüsselt werden, bevor man sie in der Cloud ablegt. Leider bieten nicht alle Anbieter von Cloud-Diensten hier eine einfache und leicht zu integrierende Lösung an. In solchen Fällen sollte man auf die Nutzung des Cloud-Speichers verzichten bzw. auf alternative Produkte setzen.

Suchbegriffe: Internetwerbung, Google Doubleclick, Google Analytics, iAd, AdBlock, Ghostery, Disconnect, Cookies, Privater Modus, Geolokalisierung, Soziale Netze, Facebook, Twitter, Google Plus, Linkedin, Cloud Dienste, iCloud, Azure, OneDrive, Office 365, Adobe Creative Cloud, iWork, Google Dienste, Dropbox, Google Drive, Amazon Cloud Drive, Telekom Mediencenter, TrueCrypt, Boxcryptor