Tipps für die Internetnutzung

Sichere E-Mail-Kommunikation
Programme zum Empfangen und Versenden von E-Mails, so genannte Mail-Clients, stellen eines der größten Sicherheitsrisiken für den Datenbestand auf Ihrem Computer dar. Daher ist es sinnvoll, einige grundlegende Maßnahmen zu ergreifen, um diese Sicherheitslücke deutlich zu verkleinern.

Informationen rund um die wichtigsten Gefahren oder Ärgernisse im Zusammenhang mit E-Mail- und Internetbenutzung haben wir für Sie im Artikel „Spam, Viren und Phishing“ zusammengestellt. Begriffe wie Spam, Viren, Würmer oder Phishing werden erklärt und Möglichkeiten zum Schutz vorgestellt.

Eine unerwünschte E-Mail – ob nun gefährlich oder nur ärgerlich – lässt sich nicht zuverlässig am Absender erkennen. So können Würmer E-Mails mit dem Absender des befallenen Rechners versenden. Erhalten Sie eine E-Mail von einer Ihnen bekannten Person, deren Sprache, Stil oder Inhalt nicht zu dieser Person passt, sollten Sie stutzig werden. Die folgenden Merkmale geben eine Orientierungshilfe zum Erkennen verdächtiger E-Mails. Indem Sie selbst beim Verfassen Ihrer E-Mail diese Punkte vermeiden, signalisieren Sie den Empfängern, dass es sich um seriöse Nachrichten handelt.

- Kein oder allgemeiner Betreff („Ihre Anfrage“)
- Keine direkte Ansprache des Empfängers
- Anhänge (Attachments) werden im Text nicht erwähnt
- Angehängte Dateien sind potentiell gefährlich

Grundsätzlich gilt das weit verbreitete Programm Outlook (Steckbrief) der Firma Microsoft als anfällig in punkto Sicherheit, unter anderem weil es Teile des Browsers Internet Explorer verwendet und so von den bekannten Sicherheitslücken dieses Programms mitbetroffen ist. Als sicher und gut konfigurierbar gelten z. B. das Open Source -Programm Thunderbird (Steckbrief) oder der mit dem Apple-Betriebssystem Mac OS X ausgelieferte Client Mail (Steckbrief). Um Ihren E-Mail-Verkehr möglichst sicher zu gestalten, sollten Sie folgende Einstellungen in dem von Ihnen verwendeten E-Mail-Client vornehmen (nicht alle Clients bieten jede dieser Einstellungsmöglichkeiten):

- Deaktivieren Sie die Möglichkeit, E-Mails im HTML -Format zu verfassen und zu empfangen. HTML kann schädliche Inhalte transportieren, es gilt daher als guter Stil, E-Mails ausschließlich als reine Textnachrichten zu versenden.
- Deaktivieren Sie die Funktion, Dateianhänge automatisch auszuführen sowie das Ausführen von JavaScript.
- Deaktivieren Sie die Möglichkeit, externe Grafiken nachzuladen. Durch den Grafikabruf können Informationen übertragen werden, die unbemerkt eine Empfangs- und Lesebestätigung versenden.

Für das Versenden sensibler Inhalte und Dokumente bietet sich eine Verschlüsselung der E-Mail mit dem kostenlosen Programm PGP (Pretty Good Privacy) an, das in den E-Mail-Client integriert werden kann, wenn eine entsprechende Schnittstelle vorhanden ist. PGP gibt es in einer kommerziellen, für Privatanwender jedoch kostenlosen Variante (www.pgp.com) sowie als Open Source-Angebot (www.gnupg.org). Eine Anleitung zur Installation von PGP finden Sie auf den Seiten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Sicherheitseinstellungen im Browser
Insbesondere der sehr weit verbreitete Browser Internet Explorer der Firma Microsoft hat immer wieder mit seinen massiven Sicherheitslücken Schlagzeilen gemacht. Ein besonders hohes Risiko birgt die ActiveX -Technologie. Diese sollte daher deaktiviert werden. Als Alternative zum Internet Explorer hat sich in letzter Zeit für Windows-Betriebssysteme der Open-Source-Browser Firefox (kostenloser Download unter www.mozilla.com) etabliert. Der

mittlerweile auch ohne Werbung kostenlos erhältliche Browser Opera, der bei vielen beliebten Funktionen wie z. B. dem Tabbed Browsing oder Mausgesten als Vorreiter gilt, genießt auch zunehmend Sympathien (www.opera.com).

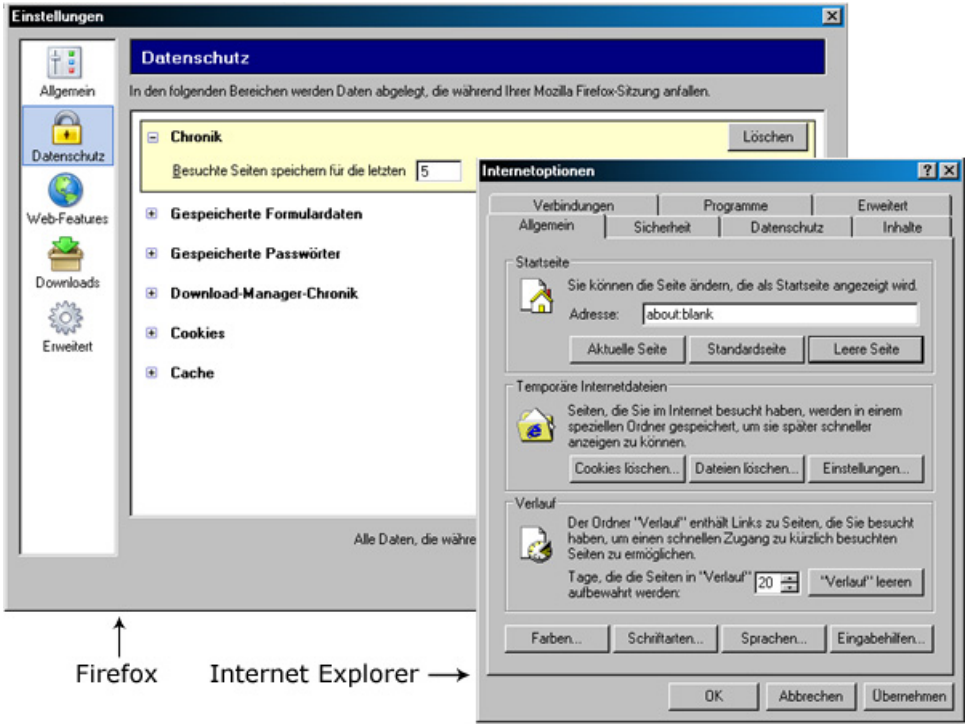
Durch einige grundlegende Einstellungen im Browser können Sie das Surfen im Internet deutlich sicherer gestalten – insbesondere auch im Hinblick auf den Datenschutz. Im folgenden haben wir für Sie die wichtigsten Konfigurationen zusammengestellt.

Halten Sie die Größe des Caches (temporäre Internetdateien) möglichst gering. Insbesondere bei schnellen Internetverbindungen (Breitband) ist der ursprüngliche Zweck dieses Zwischenspeichers, bereits besuchte Seiten schneller laden zu können, zunehmend überholt.

Unter Umständen ist es sinnvoll, den so genannten Verlauf (in Firefox: *Chronik*) regelmäßig zu leeren. Dort werden je nach Einstellung die besuchten Webseiten der letzten Tage, Wochen oder sogar Monate gespeichert. Problematisch ist dies insbesondere, wenn andere Personen Zugriff auf Ihren Rechner haben und sich so leicht über Ihre Surfgewohnheiten informieren können.

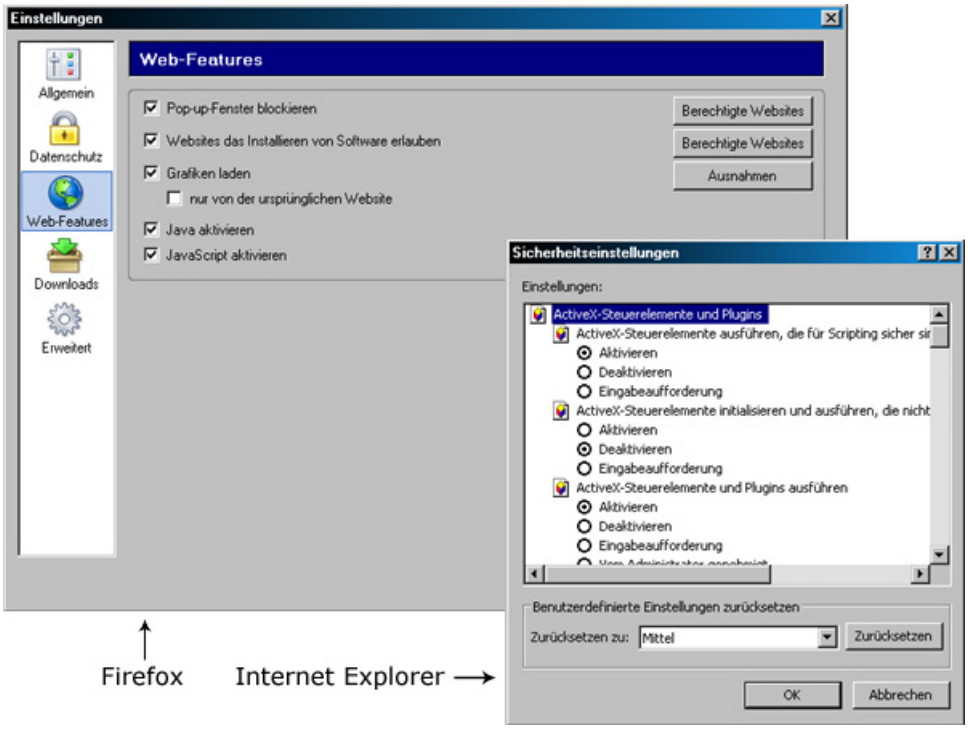
Überprüfen Sie die Behandlung von Cookies. Cookies sind keine ausführbaren Programme und können daher auf Ihrem Rechner keinen Schaden anrichten. Sie sind jedoch im Hinblick auf den Datenschutz problematisch, da sie es erlauben, Daten z. B. über Ihre Surfgewohnheiten zu sammeln. Dabei haben Sie keinerlei Kontrolle darüber, welche Informationen gesammelt und an wen diese weitergegeben werden. Langlebige Cookies (persistente Cookies) sind problematischer als so genannte Sitzungscookies (session cookies), die nach dem Schließen des Browsers gelöscht werden. Die Lebensdauer persistenter Cookies kann viele Jahre betragen, sie können eine entsprechend umfangreiche Datensammlung zusammenstellen. Sinnvoll und seriös eingesetzte Cookies können den Komfort des Surfens jedoch erhöhen, daher lassen die meisten Browser eine differenzierte Behandlung der Cookies zu. Es empfiehlt sich, Cookies mit einer längeren Lebensdauer nur auf Nachfrage zu akzeptieren oder generell abzulehnen und alle Cookies regelmäßig zu löschen.

Im Internet Explorer finden Sie die genannten Einstellungsoptionen unter *Extras> Internetoptionen> Allgemein*. Benutzen Sie Firefox, wählen Sie *Extras>Einstellungen>Datenschutz*. Unter Opera wählen Sie *Extras>Einstellungen>Erweitert>Cookies*.



Wenn Sie ganz sicher gehen wollen, deaktivieren Sie aktive Inhalte wie Java, JavaScript, ActiveX -Controls und VBScript. Aktive Inhalte sind kleine Programme, die auf Ihrem Rechner Schaden anrichten und Daten ausspionieren können.

Allerdings werden heute sehr viele Webseiten unter Verwendung aktiver Inhalte erstellt, so dass das generelle Ausschalten dieser Funktionen Sie von einem erheblichen Teil des Internet ausschließt. Ein möglicher Ausweg besteht darin, beim Besuch seriöser Seiten die entsprechenden Funktionen zu reaktivieren und anschließend wieder auszuschalten. Im Internet Explorer finden Sie diese Einstellungsoptionen unter *Extras> Internetoptionen> Sicherheit> Stufe anpassen*. Benutzen Sie Firefox, wählen Sie *Extras > Einstellungen> Web-Features*. Unter Opera wählen Sie *Extras>Einstellungen>Erweitert>Inhalte*.



Bei den diversen Sicherheitseinstellungen sollte die Faustregel gelten, so viele Funktionen wie möglich zu deaktivieren oder zumindest nur auf Nachfrage zuzulassen. Achten Sie darauf, Ihren Browser durch Updates oder das Installieren einer neueren Version aktuell zu halten.

Techniken zur Anonymisierung der Internetnutzung
Möchten Sie vermeiden, allzu aussagekräftige Datenspuren im Internet zu hinterlassen, können Sie auf verschiedene Techniken zurückgreifen, mit denen sich der Datenschutz beim Surfen im Internet weiter verbessern lässt. Es kann jedoch nie ein hundertprozentiger Schutz garantiert werden. Insbesondere im Rahmen der NSA-Enthüllungen wurde bekannt, dass verschiedene Aktivitäten von Geheimdiensten darauf abzielen, Nutzer von Anonymisierungsdiensten zu identifizieren und zu belauschen. Zumindest im Falle des TOR-Projektes scheinen sich aber die grundsätzlichen Sicherheits-Funktionen zu bewähren. So räumte die NSA in durch den Guardian veröffentlichten internen Dokumenten unter dem Punkt "Tor Stinks..." ein, durch manuelle Verfahren lediglich einen minimalen Teil der Tor-Nutzer identifizieren zu können.

- Tor stellt auf Basis von Open Source-Software ein Netzwerk zur Anonymisierung von Verbindungsdaten bereit. Insbesondere beim Surfen im Internet können sich Nutzer vor der Analyse ihres Datenverkehrs schützen.
- Der Dienst AN.ON Online bietet über die kostenlose Software JAP individuellen Nutzern die Möglichkeit, sich anonym im Internet zu bewegen. Dies geschieht über den Einsatz von Proxyservern, die zwischen den Server einer aufgerufenen Webseite und den Computer des Nutzers (Client) geschaltet werden. Gegenüber dem Webserver tritt der Proxyserver als Client auf und schützt so die Identität des Nutzers. Im Rahmen des AN.ON-Dienstes wird dieser Schutz durch den Einsatz von Verschlüsselungen und so genannter Mix-Netze ausgebaut. Nähere Informationen sowie die Möglichkeit zum Download der benötigten Software finden Sie unter anon.inf.tu-dresden.de.
- Die kostenlose Plattform P3P (Platform for Privacy Preferences) ist durchdas WWW-Consortium (W3C) standardisiert und unterstützt den Internetsurfer dabei, die Kontrolle über seine persönlichen Daten zu behalten. P3P ermöglicht einen schnellen Zugriff auf die Datenschutzinformationen einer Webseite. Mit einem P3P-kompatiblen Browser (z. B. Firefox, Internet Explorer) kann zudem nach entsprechender Konfiguration die

Annahme von Cookies gesteuert werden. Umfangreiche Informationen zu P3P sowie Anleitungen zur Installation für verschiedene Browser finden Sie auf den Seiten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Letzte Änderung: 11.06.2015

Zitation

e-teaching.org (2015). Tipps für die Internetnutzung. Zuletzt geändert am 11.06.2015. Leibniz-Institut für Wissensmedien: https://www.e-teaching.org/technik/datenhaltung/datenschutz/tipps_internetnutzung/index_html. Zugriff am 24.05.2019