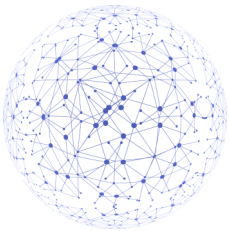
IT-Sicherheitstipp Nr.1 – März 2019

Sicherer Surfen im Internet



Was ist das Internet?

Das Internet ist ein weltumspannendes Netz von Millionen von Rechnersystemen. Als offenes Datennetz ist es grundsätzlich für jedermann zugänglich.
Eine zentrale Verwaltung der Inhalte gibt es nicht. Das heißt: Es ist nicht klar zu bestimmen, aus welchen Quellen Informationen im Internet stammen und ob sie richtig sind. Insbesondere bei sensiblen Daten sollte man im Internet große Vorsicht walten lassen. Außerdem ist bei der unverschlüsselten Übertragung von Informationen nicht klar, wer alles mitlesen kann.

Vertrauenswürdigkeit von Webseiten

Haben Sie sich schon mal Gedanken darüber gemacht, wer eine Webseite veröffentlicht und wer für den Inhalt verantwortlich ist?
Diese Fragen sind mit letzter Sicherheit oft nur schwer zu beantworten. Viele Informationen erscheinen im Internet anonym und ungeprüft. Die technisch leicht mögliche automatische Weiterleitung auf andere Web-Server macht es Ihnen zudem schwer, die Kontrolle zu behalten.

So verhalten Sie sich richtig:

- Recherchieren Sie nur in vertrauenswürdigen Quellen (z.B. Online-Präsenzen von renommierten Printmedien oder moderierten Lexika)
- Bleiben Sie kritisch gegenüber allen Informationen, die Sie im Internet finden
- Fragen Sie sich immer, wer für den Inhalt verantwortlich ist und ob Sie dieser Person vertrauen können

Der gläserne Mensch

Stetig werden neue Technologien entwickelt, um Inhalte attraktiver, schneller und dynamischer zu präsentieren. Dabei werden auch Methoden entwickelt, um Ihr Surf-Verhalten zu speichern und zu analysieren. Unsichtbar laufen Programme ab, die Sie aushorchen, beeinflussen oder sogar in die Irre führen sollen.

Deshalb gilt:

- Surfen Sie bewusst und bedenken Sie jeden "Klick"
- Speichern Sie Informationen möglichst nur aus vertrauenswürdigen Quellen
- Laden Sie keine Programme an Ihrem dienstlichen Computer aus dem Internet herunter

Technische Webinhalte

Webseiten sollen möglichst ansprechend und benutzerfreundlich sein. Das führt zur häufigen Verwendung so genannter dynamischer oder aktiver Inhalte, die auf bestimmte Internet-Technologien zurückgreifen:

- *Cookies* sind Textdateien, die von Internetseiten auf Ihrem Computer automatisch gespeichert werden, um Sie bei einem erneuten Besuch wieder zu erkennen und ggf. Nutzerprofile zu bilden
- *Plugins* ermöglichen die direkte Darstellung von Multimedia-Daten wie Klänge und Filme im Browser
- Programmtechniken wie *ActiveX, Java oder JavaScript* können Aktionen und fremde Programme direkt auf Ihrem Rechner ausführen.

So schützen Sie Ihren Computer gegen den Missbrauch durch technische Webinhalte:

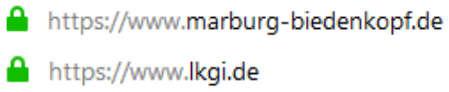
- Ändern Sie nicht selbstständig die Sicherheitseinstellungen Ihres Browsers
  (Hinweis: In den meisten Verwaltungen ist eine sichere Konfiguration des Browsers fest vorgegeben)
- Starten Sie keine Programme aus Webseiten, sofern Sie nicht dienstlich dazu angehalten werden

- Prüfen Sie Zertifikate für eine mögliche Verschlüsselung und vertrauen Sie nur den zertifizierten Stellen, die Sie kennen. Manchmal wird eine Fehlermeldung mit dem Hinweis angezeigt, dass ein Problem mit dem Sicherheitszertifikat einer Website vorliegt.
- Das Zertifikat einer Website ermöglicht das Herstellen einer sicheren Verbindung mit der Website. Zertifikatfehler treten auf, wenn ein Problem mit einem Zertifikat oder der Verwendung eines Zertifikats durch den Webserver vorliegt. Sie sollten Zertifikatswarnungen genau durchlesen und nicht einfach überspringen.

Verschlüsselter Zugriff auf Webseiten

Neben allgemein zugänglichen Webseiten gibt es häufig Seiten, deren Inhalt nur für bestimmte Personen lesbar sein soll. Um auf diese Seiten zuzugreifen, müssen meist geheime Zugangsdaten wie Benutzername und Passwort oder Kontonummer und PIN eingegeben werden.
Damit Zugangsdaten und Seiteninhalte bei der Übertragung im offenen Internet nicht von Dritten mitgelesen werden können, wird für die Übertragung zusätzlich das Protokoll "TLS" (Transport Layer Security) verwendet. Entsprechende Angebote erkennen Sie u.a. an der der Adresse vorangestellten Abkürzung "https".

Zu allen Seiten, deren Adresse mit https:// beginnt, baut der Browser automatisch eine verschlüsselte Verbindung auf. So wird sichergestellt, dass bei der Übertragung grundsätzlich keine Daten mitgelesen oder verändert werden können.



Die meisten Webbrowser zeigen eine verschlüsselte Verbindung durch ein entsprechendes Symbol an, häufig durch ein kleines Vorhängeschloss in der Adresszeile.

Verschlüsselte Verbindungen im Internet werden über Digitale Signaturen abgesichert. Die Ausstellung und Überprüfung digitaler Signaturen sind technisch komplizierte Prozesse. Sie werden jedoch von den Webbrowsern weitgehend automatisch erledigt, Sie können dies aber auch selbst versuchen.

Blocken krimineller Seiten

Einige Verwaltungen stellen mit Hilfe von zentralen Filtersystemen sicher, dass Webseiten mit extremistischen, pornografischen und vergleichbaren Inhalten automatisch geblockt werden. Davon unabhängig sollten Sie von sich aus Internetangebote meiden,

- die strafbare bzw. rechtswidrige Inhalte haben,
- die andere Personen am Arbeitsplatz belästigen oder – insbesondere minderjährige Kolleginnen und Kollegen – verstören können,
- die keinen dienstlichen Bezug haben, insbesondere wenn Ihnen die private Internetnutzung untersagt ist

Verwaltungsspezifische Richtlinien zur Internetnutzung

Viele Verwaltungen legen konkrete Richtlinien für die Internetnutzung fest.
Diese regeln zum Beispiel:

- die private Nutzung von Internet-Diensten
- den Umgang mit schützenswerten und vertraulichen Daten
- die Verantwortung der Beschäftigten für Datenschutz und Datensicherheit
- Verbote der Installation von Software
- Verbote von Einrichtung und Betrieb nicht-genehmigter Internet-Zugänge
- die Protokollierung von E-Mail- und Internet-Nutzung

Zur Aufrechterhaltung des Betriebs oder zur Fehleranalyse muss der Internetverkehr in bestimmten Situationen protokolliert werden.