



Sicher im Internet

Tipps zum Selbstschutz

Auf diesen Seiten finden Sie Hinweise und Tipps, wie Sie Ihren Aufenthalt im weltweiten Datennetz sicherer gestalten können.

Dabei geht es nicht um die angebliche Sicherheit mit einem Klick. Vielmehr soll gezeigt werden, welche Bereiche zum Selbstschutz im Netz in Betracht kommen, welche Werkzeuge es gibt und welche Fallstricke dabei lauern können.

Die Informationen gliedern sich dabei in drei Bereiche:

- **Absichern des eigenen Rechners**
- **Verschlüsseln der Kommunikation**
- **Vermeiden von Datenspuren**

Mit freundlicher Genehmigung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), <http://www.datenschutzzentrum.de>



Absichern des eigenen Rechners

- **Zugangsschutz:** Passwörter, Dateisysteme und Firewalls
- **Integrität der Software:** Viren, Würmer und Dialer
- **Konfiguration:** Browser, Mailprogramm und Active Content
- **Ausrüstung:** Zusatztools mit Zusatznutzen

Absichern des eigenen Rechners

Beim Bemühen um Sicherheit im Internet ist zuerst wichtig, einen Blick auf den eigenen PC zu werfen. Erst wenn einige Grundvoraussetzungen erfüllt sind, machen Maßnahmen wie Verschlüsselung oder Anonymisierung Sinn.

Zuerst gilt unser Augenmerk dem Zugriff auf den eigenen Rechner. Wer kommt hierfür in Frage? Die Möglichkeiten reichen hier von der kleinen Schwester über den Bekannten, der im Urlaub Blumen gießt bis hin zum Einbrecher. Und der kann durch die Tür wie auch über das Internet kommen. Der Zugang zum PC muss also sowohl für Hard- als auch für die Software geregelt sein. Es wäre fatal, sich durch verschlüsselt verschickte eMails in Sicherheit zu wiegen, wenn ein dritter heimlich am eigenen PC die Post liest - unverschlüsselt.

Geeignete Maßnahmen für den Zugangsschutz reichen hier von der physischen Sicherung des PCs bis zum Schutz vor Eindringlingen aus dem Netz durch eine PC-Firewall.

Gleichzeitig gilt es, die verwendete Software "sauber" zu halten. Hat sich erst einmal ein Virus oder Trojaner auf dem eigenen PC eingenistet, wird es knifflig: Angriffe von Innen sind schwerer abzuwehren.

Nicht zuletzt muss die verwendete Software möglichst sicher konfiguriert sein. Browser, eMail-Programm, Firewall und Anwendungsprogramme wollen richtig eingestellt sein, um maximalen Surfspaß bei minimalem Risiko zu ermöglichen. Leider sind die Programme in der Regel im Auslieferungszustand unter Datenschutzaspekten mangelhaft eingerichtet.

Wir zeigen Ihnen, wie Sie mit wenigen Handgriffen die gängigen Programme abschotten und so entspannt durchs Web surfen können.

Weitere Informationen und Links:

<http://www.datenschutzzentrum.de/selbstdatenschutz/internet/absichern.htm>



Verschlüsseln der Kommunikation

- **PGP / GnuPG:** Verschlüsseln von eMails
- **Steganographie:** Verbergen von Daten
- **Webzugriffe mit SSL:** Verschlüsselt surfen

Verschlüsseln der Kommunikation

Die Absicherung des eigenen Rechners hat naturgemäß enge Grenzen und stellt nur die notwendige Grundlage des Selbstdatenschutzes dar. Spätestens, wenn persönliche oder gar vertrauliche Informationen über das Netz versandt werden sollen, endet der eigene Einfluss. Um Daten auch beim Versand über Datennetze vertraulich zu halten, bedient man sich der Verschlüsselung.

Grundsätzlich kommen dabei zwei Verfahren zum Einsatz: Die **symmetrische** und die **asymmetrische Verschlüsselung**. Bei der symmetrischen Verschlüsselung kommt zum Ver- und Entschlüsseln derselbe Schlüsselcode zum Einsatz. Das Verfahren ist schnell und effizient – und unhandlich. Mit jedem Kommunikationspartner muss ein separater Schlüssel vereinbart werden und auf einem sicheren Kanal übertragen werden.

Als Alternative bietet sich asymmetrische Verschlüsselung, die sogenannte **Public-Key-Kryptographie** an. Hier werden zum Ver- und Entschlüsseln jeweils getrennte Schlüsselcodes verwendet. Der Code zum Verschlüsseln wird öffentlicher Schlüssel genannt und kann über beliebige unsichere Kanäle übermittelt werden. Zum Entschlüsseln, also Lesen einer Nachricht, kommt der Gegenpart, der private Schlüssel zum Zuge. Dieser verbleibt beim Besitzer und wird niemals an andere übermittelt.

Beide Varianten, symmetrische wie asymmetrische Verschlüsselung haben spezielle Vor- und Nachteile. Symmetrische Verschlüsselung ist schnell zu berechnen und eignet sich daher vor allem für synchrone oder quasi-synchrone Kommunikation. Asymmetrische Verschlüsselung ist hingegen vergleichsweise zeitaufwändig zu realisieren und erfordert durch die größeren Schlüssellängen auch ein höheres Datenaufkommen.

In der Praxis kommen deshalb nahezu immer **Hybridverfahren** zum Einsatz. Dabei wird zunächst ein symmetrischer Schlüssel für die Dauer der Sitzung generiert, der sog. Session-Key. Beide



Kommunikationspartner besitzen außerdem je ein asymmetrisches Schlüsselpaar. Mit Hilfe des öffentlichen Teils eines solchen Schlüsselpaares wird nun der Session-Key codiert und zum anderen Rechner geschickt, der ihn mit seinem privaten Schlüssel dechiffrieren kann. Dieses Verfahren nutzt also die zeitaufwändige asymmetrische Verschlüsselung nur einmalig zur Übertragung des symmetrischen Session-Keys.

Weitere Informationen und Links:

<http://www.datenschutzzentrum.de/selbstdatenschutz/internet/verschluesseln.htm>



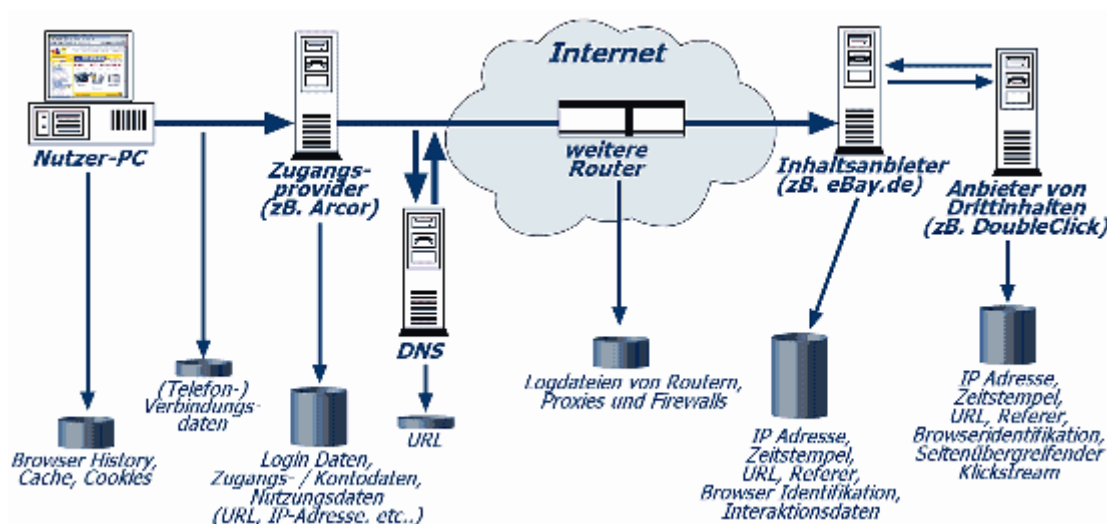
Vermeiden von Datenspuren

- **Surfspuren: Cookies & Co**
- **Selbst sichern mit P3P**
- **Anonym surfen**

Vermeiden von Datenspuren

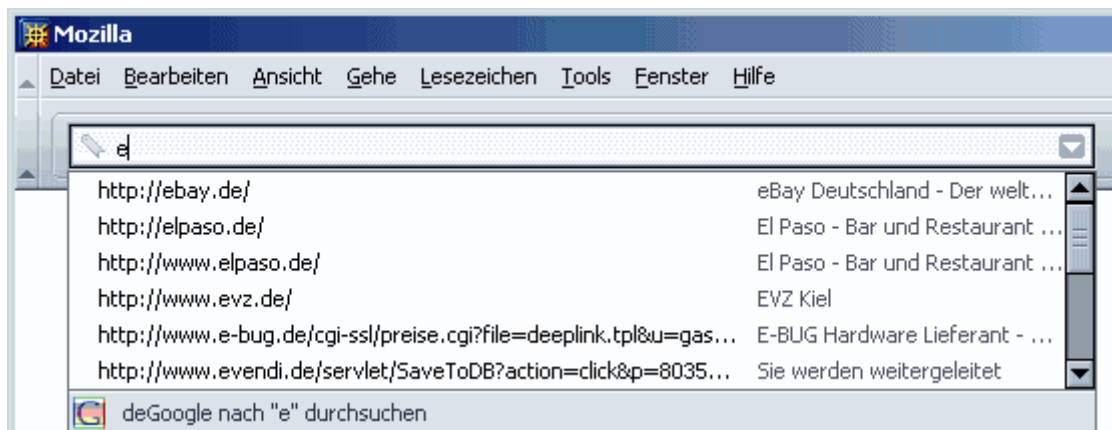
Wann, Woher, wohin - im Alltag sind diese Informationen selten ein Thema. Niemand käme auf die Idee, beim Überfliegen der Schlagzeilen am Kiosk seinen Namen zu nennen. Auch der Kioskbetreiber hat besseres zu tun, als die Verweildauer der Kunden vor seinen Zeitungen zu notieren und sich ihre Gesichter zu merken.

Im Web sind diese Vorgänge jedoch keine Seltenheit. Mehr noch: Im weltweiten Datennetz ist solch eine Datenerfassung die Regel. Und nicht nur die Anbieter von Webangeboten schreiben fleißig mit, auch dritte, von denen der Internetnutzer nicht einmal wissen muss, sammeln fleißig Daten. Viele der beim Surfen anfallenden Informationen sind dabei vermeidbar.



Nutzer-PC

Bereits der eigene Rechner protokolliert mehr, als manche Nutzer ahnen. Neben einer Liste der zuletzt besuchten Internetseiten (die sogenannte "History") werden auch Teile dieser besuchten Seiten auf der Festplatte abgelegt, um sie bei einem erneuten Aufruf schneller anzeigen zu können. Daher finden sich im sogenannten Cache-Verzeichnis vor allem die Grafiken der besuchten Seiten. Auch die Adresszeile ist bei aktuellen Browsern leistungsfähiger geworden und merkt sich vergangene Eingaben. Dadurch erscheinen bereits verwendete Webadressen nach Eingabe weniger Buchstaben und der Nutzer muss nicht die vollständige Adresse eintippen. Allerdings gewährt diese Liste schon einen interessanten Einblick in die Surfgewohnheiten.



Zugangspvoder

Der Zugangspvoder versorgt den Nutzer mit einem Zugang zum Internet. Er stellt ihm eine Verbindung zur Verfügung und weist ihm eine IP-Adresse zu. Somit fallen dort Informationen über bestehende Online-Verbindungen an. Dazu zählen Zeit und Dauer der Verbindung, die Login Daten (also Benutzername und Kennwort) sowie die zugeteilte IP-Adresse. Darüber hinaus hat der Provider natürlich Zugriff auf sämtliche Nutzungsdaten. Die aufgerufenen URLs bleiben ihm ebensowenig verborgen wie im Klartext übermittelte Passworte und eMails.

Internet (Router etc.)

Aufgerufene URLs und im Klartext übermittelte Daten können auch an jedem anderen Knotenpunkt im Internet gespeichert werden, der von einem Datenpaket passiert wird. Generell gilt, dass man nicht weiß, welchen genauen Weg ein Datenpaket zum Zielserv er nehmen wird. Da das Internet im Wortsinne ein Netz ist, gibt es verschiedene Wege zwischen zwei entfernten Netzknoten. Welchen Weg ein Datenpaket einschlägt, hängt von verschiedenen Faktoren ab, auf die der Nutzer keinen Einfluss hat. Allerdings liegen die Daten auf einem Router irgendwo im Internet nur in Verbindung mit der IP-Adresse vor. Der Betreiber des Routers kann also nur erkennen, dass Daten von einer bestimmten IP-Adresse zu einem bestimmten Zielrechner gesendet werden. Die Verknüpfung zwischen IP-Adresse und echtem Namen des Nutzers kann



nur der Provider herstellen. Sämtliche unverschlüsselten Informationen, die an den Zielservers übermittelt werden sollen, können auf einem Router jedoch ebenfalls mitgelesen werden.

Inhaltsanbieter

Der Zielservers erhält selbstverständlich die gleichen Daten wie ein Router im Internet, also IP-Adresse, Zeitstempel und URL. Hierzu zählt auch der Referer, der die zuvor besuchte Webseite angibt, ebenso wie Browserkennung und sonstige Informationen über die eigene Hard- und Software, die standardmäßig beim Surfen übermittelt werden.

Zusätzlich zu diesen Daten kann der Inhaltsanbieter darüber hinaus aufzeichnen, was der Nutzer auf seinen Seiten tut. Meldet sich der Nutzer mit einer Kennung an, beispielsweise um sich an einem Webforum zu beteiligen, entsteht ein Nutzungsprofil durch die Interaktionsspuren. Der Inhaltsanbieter kann diese Interaktionsspuren mit den zuvor beschriebenen technischen Spuren verknüpfen.

Anbieter von Drittinhalten

Als Drittinhalt bezeichnet man Webseitenelemente, die nicht vom Anbieter der Webseite selbst erzeugt werden, sondern vom Server eines dritten geladen werden. Bekanntestes Beispiel für solche Drittinhalte sind Werbebanner. Diese werden vom Anbieter einer Webseite nur als Link in die eigene Seite eingefügt, der Browser des Nutzers lädt das Banner dann vom Rechner des Drittanbieters nach. Bei diesem Nachladevorgang baut der eigene Rechner eine Verbindung zum Server des Drittanbieters auf, wo auf diese Weise erneut sämtliche technischen Spuren (IP-Adresse, Browserinformationen etc.) anfallen. Der Anbieter von Drittinhalten kann kein Nutzungsprofil aufgrund von Interaktionsspuren bilden, er kann jedoch den Klickstream aufzeichnen. Da sein Werbebanner jedesmal abgerufen wird, wenn eine damit verknüpfte Webseite angesurft wird, kann ein solcher Werbeserver recht genau nachverfolgen, welchen Weg der Inhaber einer bestimmten IP-Adresse durch das Netz nimmt. Durch das Setzen eines Cookies kann er darüber hinaus den Weg durchs Web auch dann weiter verfolgen, wenn sich die IP-Adresse ändert.

Weitere Informationen und Links:

<http://www.datenschutzzentrum.de/selbstdatenschutz/internet/datenspuren.htm>