anonym surfen

Der Whistleblower Edward Snowden hat aufgezeigt, dass die Kommunikationsmittel des 21. Jahrhunderts dem Schutz der Privatsphäre in manchen Fällen nicht zuträglich sind. Dass aber nicht nur Geheimdienste oft mehr wissen als die engsten Freundinnen und Freunde oder manchmal auch man selbst, kann beispielsweise jeden Tag an Werbebannern beobachtet werden, die einem auf Webseiten präsentiert werden. Andererseits können diese auch hilfreich sein, wenn sie etwa passende Hotels zum soeben gebuchten Städteflug vorschlagen. Oftmals werden persönliche Daten als Gegenleistung für Gratisangebote freiwillig hergegeben. Dennoch möchten die meisten Nutzerinnen und Nutzer ihre Daten (im Internet) schützen und ihre Privatsphäre wahren.

Anonymität & Privatsphäre

IP-Adressen

Die IP-Adresse ist ein Zahlencode, der einem Gerät, das ans Netz angebunden ist, entweder fix zugewiesen oder vom Provider dynamisch vergeben wird. IP-Adressen werden verwendet, um Daten von einem absendenden Gerät zu einem empfangenden Gerät zu transportieren, sie funktionieren also wie Telefonnummern, die Absenderinnen oder Absender und Empfängerinnen oder Empfänger eindeutig identifizieren. Eine IP-Adresse wird einem Computer zugewiesen, der in ein Netz eingebunden ist, dadurch wird er adressierbar und somit erreichbar. Geräte hinter Firewalls oder ***ROUTERN*** haben dabei vom Internet aus gesehen oftmals nur eine gemeinsame Internetadresse, sind also anhand der IP-Nummer nicht unterscheidbar. Das aktuell weltweit eingesetzte Internetprotokoll ist ***IPV4***. IPv4 soll aber in den kommenden Jahren durch ***IPV6*** abgelöst werden, da dieses eine deutlich größere Zahl an Adressen ermöglicht.

Der private Modus

Die meisten Webbrowser bieten in ihren Einstellungen die Möglichkeit des „InPrivate"-Surfens. Dieser private Modus sorgt dafür, dass beim Internetsurfen keine bzw. weniger Spuren hinterlassen werden. Beispielsweise werden hierbei die Adressen der aufgerufenen Internetseiten nicht gespeichert und nicht in einer Chronik dokumentiert, Sucheinträge, Cookies und temporäre Internetdateien nicht gespeichert. Der private Modus ermöglicht, dass Nutzerinnen und Nutzer anonym(er) surfen können, kann aber keine absolute Anonymität garantieren. Empfehlenswert ist der private Modus besonders bei der Nutzung von fremden oder öffentlichen Computern.

- → ***Google Chrome:*** *Einstellungen > Neues Inkognitofenster*
- → ***Internet Explorer:*** *Einstellungen > Sicherheit > InPrivate-Browsen*
- → ***Mozilla Firefox:*** *Einstellungen > Privates Fenster*
- → ***Opera:*** *Fenster und Tabs > Neuer Privater Tab*
- → ***Safari:*** *Menü > Privates Surfen*

Router:

Netzwerkgeräte, die Informationspakete zwischen mehreren Rechnernetzen weiterleiten können. Sie werden u. a. für die Internetanbindung verwendet.

IPv4 bzw. Internet Protocol Version 4:

Aktuelles Internetprotokoll, das die technische Grundlage des Internets bildet. IPv4-Adressen sind 32 Bit lang.

IPv6 bzw. Internet Protocol next Generation (IPnG):

Neues Internetprotokoll, das IPv4 ablösen soll. IPv6-Adressen sind 128 Bit lang.

Firewall:

(Engl. für Brandwand oder Brandschutz.) Sicherungssystem, das einzelne Computer oder Netzwerke vor unerlaubten Zugriffen schützt.

Anonymizer

Server:
Computer, auf dem Programme laufen, auf die andere Computer (Clients) zugreifen können.

Client:
Computerprogramm, das auf einem Endgerät installiert ist und bestimmte Dienste vom Server abrufen kann.

Proxy:
(Engl. für Stellvertreter.) Schnittstelle in einem Netzwerk, die die Kommunikation zwischen zwei Servern/Rechnern weiterreicht.

Web Proxy Autodiscovery Protocol bzw. WPAD:
Protokoll, mit dem Web-Clients automatisch verfügbare Proxys finden können.

Virtual Private Network bzw. VPN:
(Engl. für virtuelles privates Netzwerk.) Schnittstelle in einem Netzwerk; kann eine Verbindung zwischen zwei Netzwerken sein oder zu einem bestimmten Service.

Um für mehr Anonymität zu sorgen, gibt es verschiedene Tools, die unterschiedlich viel technisches Know-how erfordern. Eine Möglichkeit sind hierbei Anonymisierungsprogramme, die die Internetverbindung eines Geräts über einen Anonymisierungsserver lenken. Dadurch wird die wahre Herkunft – also die IP-Adresse – gegenüber dem Zielserver verschleiert. Die gängigsten Varianten hierfür sind Proxy-Server oder Virtual Private Networks (VPN).

Der Proxy-***SERVER*** ist eine Schnittstelle in einem Netzwerk, die eine Vermittlerfunktion innehat. Vereinfacht formuliert nimmt ein ***PROXY*** auf der einen Seite Anfragen entgegen und leitet sie über seine eigene Adresse an die Zieladresse weiter (quasi wie eine Umleitung oder eine Zwischenstation); die Adresse des einen bleibt bei einer Proxy-Umleitung dem anderen verborgen, was eine gewisse Anonymität ermöglicht. Proxys werden aber nicht nur zur Schaffung von mehr Privatsphäre eingesetzt, sondern beispielsweise auch zum Schutz von Servern oder ***CLIENTS***. In diesem Zusammenhang werden Proxys zum Beispiel als Schnittstelle bzw. „Torhüter" zwischen einem privaten Netzwerk (z. B. Intranet einer Firma) und einem öffentlichen Netzwerk (Internet) verwendet, was das private Netzwerk weniger angreifbar macht.

Proxys sind meistens im Zusammenhang mit der Umleitung der Internetzugriffe des Browsers interessant. Mit einem WPAD-Protokoll können Web-Clients automatisch zu verwendende ***WEB-PROXYS*** innerhalb eines Computernetzwerks finden. Mit WPAD können alle Web-Clients angewiesen werden, Proxy-Server zu verwenden. Das wird von den Browsern Mozilla Firefox, Google Chrome und Internet Explorer unterstützt.

Ein ***VIRTUAL PRIVATE NETWORK (VPN)*** ist eine Schnittstelle in einem Netzwerk. VPN-Verbindungen finden in verschiedenen Formen Anwendung. Ein gängiges Beispiel hierfür ist die Verbindung von einem Netzwerk zum anderen via VPN-Zugang, der quasi einen Tunnel zwischen diesen beiden bildet. Beispielsweise, wenn eine Mitarbeiterin oder ein Mitarbeiter von zu Hause aus Zugriff auf das Firmennetz bekommt. Eine andere Variante des Virtual Private Network ermöglicht einen Fernzugriff auf bestimmte Anwendungen, ohne eine direkte Anbindung an das entsprechende Netzwerk.

Anonym surfen

Wer mit Webbrowsern im Internet surft, hinterlässt Spuren, die von den Diensteanbieterinnen und -anbietern (Webseiten, Suchmaschinen, Mail-Dienste) gesammelt werden können, um beispielsweise Profile im Hinblick auf die Aktivitäten zu erstellen. Selbst wenn Cookies oder andere Spuren im Browser gelöscht werden, bleibt immer noch die IP-Adresse, die das Endgerät oder das Netz, an dem dieses hängt, eindeutig identifiziert. Es gibt aber zahlreiche Services, die sich Anonymität und Datenschutz auf die Fahnen geschrieben haben. Sie werben damit, keine Daten über ihre Nutzerinnen und Nutzer zu sammeln, es werden also keine Logdateien mit anwenderbezogenen persönlichen Daten gespeichert. Die bekanntesten Suchmaschinen sind DuckDuckGo, Ixquick und Metager.

Nutzerinnen und Nutzer müssen sich hierbei aber darüber im Klaren sein, dass die Auswertung anwenderbezogener Daten beispielsweise für „relevantere" Suchergebnisse sorgen kann. Suchen Nutzerinnen und Nutzer aus Österreich nach einem Begriff, werden ihnen zum Beispiel eher Artikel österreichischer Medien angezeigt. Wird nach einem Geschäft gesucht, erscheinen eher jene in der eigenen Umgebung.

www.duckduckgo.com
www.Ixquick.com
www.metager.de

Das Tor Netzwerk

Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Hierbei wird der Datenverkehr durch verschiedene zwischengeschaltete Server geleitet, sodass die Verbindungsdaten bzw. die Absenderin oder der Absender nicht mehr nachvollziehbar sind. Dieses Netzwerk kann für verschiedene Dienste genutzt werden, oft etwa zum Internetsurfen, für E-Mail-Verkehr, Instant Messaging oder ***P2P***.

Nutzerinnen und Nutzer können den Tor-Browser für Windows-Betriebssysteme kostenlos auf der Webseite www.torproject.org downloaden. Das anonyme Surfen über das Tor-Netzwerk funktioniert mittels Onion Proxy Client. Nutzerinnen und Nutzer installieren diesen Client auf ihrem Endgerät. Dieses Programm verbindet sich mit dem Tor-Netzwerk und erhält eine Liste mit verfügbaren Tor-Servern. Für jede Suchanfrage wählt der Client eine zufällige Verbindung über drei verschiedene Server, wodurch größtmögliche Sicherheit und Anonymität garantiert werden. Dieser Verbindungsaufbau wird in regelmäßigen Abständen wiederholt.

www.torproject.org

Peer-to-Peer bzw. P2P:
Verbindungsart, bei der direkt von Teilnehmerin oder Teilnehmer zu Teilnehmerin oder Teilnehmer übertragen wird.

Achtung
Nutzerinnen und Nutzer müssen sich bewusst sein, dass Tor kein Garant für völligen Datenschutz und mehr Privatsphäre im Internet ist. Beispielsweise gab es dieses Jahr einen größeren Angriff auf das Tor-Netzwerk bzw. die Anonymisierungsknoten, sodass teilweise nachvollzogen werden konnte, wer welche Tor-Dienste genutzt hat. Userinnen und User laufen zudem Gefahr, stärker überwacht oder sogar ausspioniert zu werden. Die NSA hat viele Nutzerinnen und Nutzer genau aus dem Grund beobachtet, dass sie Dienste über das Tor-Netzwerk in Anspruch genommen hatten.

Cookies

Cookies haben trotz ihres harmlosen Namens keinen guten Ruf. Sie sind Teil von Webseiten, speichern für verschiedene Funktionen notwendige Daten und hinterlegen diese auf dem Computer oder mobilen Endgerät. Mit diesen Datenkrümeln können Userinnen und User beim (wiederholten) Besuch einer Webseite wiedererkannt werden und die Webseiten-Betreiberinnen und -Betreiber können mittels der gesammelten Informationen ein Profil erstellen. Das hört sich im ersten Moment schlimmer an, als es ist, denn mittels Cookies kann die Webseite für jeden Besuch individuell angepasst werden. Die Verwendungsmöglichkeiten reichen dabei von Online-Einkaufswagen über automatische Sprach- und Ländereinstellungen bis hin zu personalisierter Werbung.

Firefox:
Einstellungen > Datenschutz > Chronik „niemals anlegen“

Safari:
Einstellungen > Datenschutz > Cookies blockieren

Internet Explorer:
Einstellungen > Sicherheit

Google Chrome:
Einstellungen > Erweiterte Einstellungen > Datenschutz > „Speicherung von Daten für alle Webseiten blockieren“

- → ***Firefox:*** *Einstellungen > Datenschutz > Chronik „niemals anlegen“*
- → ***Safari:*** *Einstellungen > Datenschutz > Cookies blockieren*
- → ***Internet Explorer:*** *Einstellungen > Sicherheit*
- → ***Google Chrome:*** *Einstellungen > Erweiterte Einstellungen > Datenschutz > „Speicherung von Daten für alle Webseiten blockieren“*

Wie mit Cookies umgegangen werden soll, kann ohne großen Aufwand über den Webbrowser eingestellt werden. Zusätzlich gibt es spezielle Browser-Erweiterungen ***(ADD-ONS)***, die optional installiert werden können. Empfehlenswert sind in diesem Zusammenhang die Add-ons, die Online-Werbeanzeigen blockieren (Ad-Blocker). Beim ***INTERNET EXPLORER*** können Nutzerinnen und Nutzer über eine Tracking-Schutzliste festlegen, welche Webseiten ihre Daten abfragen und ihre Online-Aktivität nachverfolgen dürfen. Auch bei anderen Browsern wie ***MOZILLA FIREFOX*** (beispielsweise NoScript, BetterPrivacy) oder ***GOOGLE CHROME*** (Ghostery, AdBlock Plus) gibt es verschiedene Add-ons, die für mehr Datenschutz sorgen. Jedoch ist auch bei Add-ons Vorsicht geboten,

Add-on:
(Engl. für Erweiterung.) Add-ons sind optionale Module, die Software oder Hardware erweitern und neue Funktionen ermöglichen.

sie sind nicht nur Hilfsmittel, sondern können unter Umständen Sicherheitsrisiken sein (siehe „Sicherheitsrisiken minimieren“, S. 84).

Daten im Internet löschen

Die beste Möglichkeit, für mehr Privatsphäre und Datenschutz zu sorgen, ist, präventive und proaktive Maßnahmen zu setzen, konkret zum Beispiel Cookies zu deaktivieren oder sich überhaupt bewusst zu machen, dass (Daten-) Spuren im Netz zurückgelassen werden.

Der erste Schritt zu mehr Kontrolle über die eigenen Daten ist, überhaupt in Erfahrung zu bringen, welche Daten vorhanden sind. Facebook bietet in diesem Zusammenhang seinen Nutzerinnen und Nutzern unter dem Menüpunkt „Einstellungen“ die Möglichkeit, eine Kopie der eigenen Facebook-Daten (z. B. Profilinformationen, Aktivitätenprotokoll, verwendete Apps, Klicks auf Werbeanzeigen) herunterzuladen. Bei Google wiederum haben Userinnen und User die Möglichkeit, auf dem ***DASHBOARD*** ihres Kontos etwa ihre Suchverläufe einzusehen und sie auch zu löschen; dies ist auch bei Bing möglich. Informationen im Internet zu veröffentlichen ist heutzutage so leicht wie noch nie. Die Schwierigkeit ist eher, die Informationen wieder wegzubekommen. Denn sind Informationen, Fotos oder sonstige Beiträge erst einmal in Umlauf, können sie über das gesamte Netz verteilt werden. Sie zu finden und wieder einzusammeln ist keine leichte Aufgabe. Finden sich im Internet unangenehme oder sensible Daten über Nutzerinnen und Nutzer, ist es zwar nicht immer leicht, sie wieder zu entfernen, es gibt aber dennoch ein paar Möglichkeiten.

Dashboard:
(Engl. für Armaturenbrett.) Je nach Onlinedienst ist es unterschiedlich ausgestaltet, meistens jedoch die persönliche Start- oder Admin-Seite, auf der Information zusammengetragen wird.

Was können Userinnen und User tun?

- → ***Die Worst-Case-Frage:*** *Es kann hilfreich sein, sich vor jedem Posting die Frage zu stellen, welche Auswirkungen „der schlimmste Fall“ hätte, wenn also das Posting oder das Foto in Umlauf geriete und auch Jahre später noch online und für andere auffindbar wäre. Der Blick in die Zukunft und der Gedanke daran, dass zukünftige Arbeitgeberinnen oder Arbeitgeber, Bekannte oder Partnerinnen und Partner ein spezielles Stück Information sehen könnten, ist oft eine gute Entscheidungshilfe vor dem Posten und Veröffentlichen.*
- → ***Personenbezogene Daten:*** *Besonders mit persönlichen Daten – Geburtsdatum, Telefonnummer, Adresse etc. – sollten Userinnen und User vorsichtig umgehen.*
- → ***Trennung von Arbeit und Vergnügen:*** *Es empfiehlt sich, die beruflichen Online-Aktivitäten von den privaten zu trennen. Für soziale Netzwerke,*

Gewinnspiele und Newsletter sind eigene E-Mail-Adressen und Nicknames von Vorteil. Der Klarname sollte dem professionellen Auftritt vorbehalten bleiben.

- → ***Soziale Netzwerke:*** *Vor allem bei sozialen Netzwerken sollten Userinnen und User unbedingt die Privatsphäre-Einstellungen im Auge behalten und gegebenenfalls die höchstmögliche Privatsphärestufe wählen.*
- → ***Webseiten Dritter:*** *Sind Informationen tatsächlich auf fremden Webseiten gelandet oder wurden anderweitig verbreitet, können sich Userinnen und User an die Webseiten-Betreiber wenden und um die Entfernung der Information bitten.*
- → ***Regelmäßige Kontrolle:*** *In regelmäßigen Abständen sollten Userinnen und User mittels Suchmaschinen das Internet nach Einträgen von und über sich selbst durchsuchen. Somit können rechtzeitig Schritte in die Wege geleitet werden, falls bei einer dieser Suchen negative Einträge gefunden werden. Um den eigenen Namen zu suchen, sollte er unter Anführungszeichen gesetzt werden, sodass die Suchmaschine nicht lediglich nach den einzelnen Wörtern sucht (z. B. „Monika Musterfrau").*

Suchmaschinen-Ergebnisse

In einem Urteil vom Mai 2014 entschied der EuGH, dass Suchmaschinen dazu verpflichtet werden können, Artikel mit veralteten oder sensiblen Personendaten aus ihren Ergebnislisten zu entfernen. Konkret müssen Verweise aus der Liste der Suchergebnisse gelöscht werden, wenn die dort aufgelisteten Informationen das Recht auf Privatsphäre und Datenschutz verletzen. Betroffene, die keine Personen des öffentlichen Lebens sind, haben laut dem EuGH einen einklagbaren Anspruch auf Löschung solcher Link-Verweise.

Ungewollte Bildaufnahmen

Laut österreichischer Rechtslage darf in öffentlichen Bereichen jede und jeder fotografieren, ebenso kann jede und jeder (ungefragt) fotografiert werden. Das gilt jedoch nicht für die Verbreitung der Aufnahmen. Sie ist nur dann erlaubt, wenn sie nicht die berechtigten Interessen der Abgebildeten verletzt. Somit sollte ein Einverständnis für die Veröffentlichung der Aufnahmen eingeholt werden. Beispielsweise müssen Club- und Partyfotografinnen oder -fotografen die Gäste vor dem Fotografieren um ihre Erlaubnis fragen, wenn das in der Praxis auch eher informell passiert.

Recht am eigenen Bild

Im österreichischen Urhebergesetz ist das Recht am eigenen Bild verankert, das ein besonderer Teil des Persönlichkeitsrechts ist. Bereits die Herstellung eines Bildes ohne Einwilligung der oder des Abgebildeten kann als Eingriff in die Persönlichkeitsrechte gelten. Fotos, Videos oder deren Begleittext dürfen nicht die berechtigten Interessen der darauf abgebildeten oder darin beschriebenen Personen verletzen. Die Aufnahmen dürfen die Abgebildeten nicht herabsetzen oder bloßstellen. Relevant bei der Bestimmung der Rechtsverletzung ist hier, ob das Bild objektiv nachteilig ist und nicht nur als solches empfunden wird. Ein Foto mit unvorteilhafter Frisur stellt somit keine Rechtsverletzung dar.

Wird ein nachteiliges Bild oder Video entdeckt, haben Userinnen und User das Recht auf Löschung oder Entfernung, da hier das Recht am eigenen Bild gilt. In vielen sozialen Netzwerken gibt es hierfür bereits standardisierte Meldeverfahren, im Rahmen derer die Nutzerinnen und Nutzer solche Bilder melden können.

Was können Nutzerinnen und Nutzer machen?

- → ***Beweissicherung:*** *Mittels Screenshots der jeweiligen Webseiten sollten Beweise gesichert werden.*
- → ***Kontaktaufnahme:*** *Als Nächstes sollte schriftlich diejenige Person kontaktiert werden, die das Foto/Video hochgeladen hat. Allenfalls können auch die Webseiten-Betreiberinnen oder -Betreiber kontaktiert werden.*
- → ***Unterlassungsklage:*** *In schwerwiegenden Fällen können Userinnen und User ihre Ansprüche auch per Unterlassungsklage und – bei Schädigung – Schadenersatzforderung vor Gericht einklagen.*
- → ***Achtung:*** *Trotz Löschung auf einer Seite kann es natürlich passieren, dass die besagten Inhalte bereits anderswo im Internet gelandet sind.*

Recht am eigenen Bild:

§78 des UrhG; schützt die Abgebildeten vor ungewollter Veröffentlichung.

Internet-Ombudsmann:

Berät in schwierigen Fällen.

www.ombudsmann.at