Themen

Geotargeting (Geolocation)

Auf dem Smartphone mit ortsbezogenen Informationen versorgt zu werden, gehört für viele Nutzerinnen und Nutzer zum Alltag. Doch auch am Computer öffnet sich die internationale Website direkt in der richtigen Sprache, im Online-Shop des großen Sportartikelhändlers erscheinen Angebote der örtlichen Filiale und auf der Website über den neuen Film werden die Vorstellungen des benachbarten Kinos angezeigt.

Der Grund für diese hellseherischen Fähigkeiten des Computers sind Methoden, mit denen Internetnutzer bzw. deren Computer geografisch lokalisiert werden können. Sie werden als Geotargeting oder Geolocation bezeichnet.

Das Geotargeting wird hauptsächlich für gezielte Werbung mit regionalem Bezug genutzt. Wie bei allen anderen Varianten der personalisierten Werbung steckt natürlich auch hier die Hoffnung auf mehr Umsatz dahinter.

Doch auch das Gegenteil ist möglich. Beim so genannten Geoblocking werden die Daten aus dem Geotargeting genutzt, um Inhalte für bestimmte Regionen oder Länder zu blockieren. Das findet man beispielsweise auf YouTube oder in Livestreams von Fernsehsendern, die nur in ausgewählten Ländern verfügbar sind.

Zahlungsanbieter nutzen Geotargeting auch zur Absicherung von Bezahlvorgängen im Internet, indem sie überprüfen, ob der Standort des Nutzers mit seinen hinterlegten Angaben übereinstimmt.

Weiß Google, wo mein Computer steht?

Dass Smartphones ständig den Standort ihrer Nutzerinnen und Nutzer ermitteln und diese Daten an Unternehmen wie Google oder Apple senden, ist inzwischen weithin bekannt.

Doch dass auch der Standort des Computers im heimischen Wohnzimmer bekannt ist, ist vielen vermutlich nicht so bewusst. Grund genug, sich anzuschauen, wie das funktioniert.

Ist ein Computer mit einem Netzwerkkabel an den Router angeschlossen, kann seine öffentliche IP-Adresse ausgewertet werden. Anhand dieser Daten kann die Position des Computers aber nur auf 10 bis 20 Kilometer genau ermittelt werden.

Foto: Rudi Jahn (Pixabay)

Deutlich genauer lässt sich der Standort eines Computers ermitteln, der per WLAN mit dem Router verbunden ist. Google und andere Unternehmen haben in den letzten Jahren Datenbanken aufgebaut, in denen WLAN-Netze und Mobilfunkmasten rund um den Globus erfasst sind.

Besucht man nun eine Website, dann übermittelt der Browser die Kennung des Routers. Anhand dieser Kennung lässt sich der eigene Standort bis auf die durchschnittliche Reichweite eines Routers bestimmen, also auf etwa 30 bis 40 Meter genau.

Kann ich die Ortung verhindern?

Auch wenn es schwierig ist, es komplett zu unterbinden, gibt es doch Möglichkeiten, den Datensammlern die Arbeit etwas schwerer zu machen.

In allen Browsern lässt sich mit Hilfe der Einstellungen die Weitergabe des eigenen Standorts an Websites blockieren. Auch in Windows 10 ist es möglich, die Position (Ortung) zu deaktivieren.

Damit ist es dann zumindest nicht mehr ganz so einfach, den Computer mit Hilfe der WLAN-Kennung zu orten.

Geotargeting (Geolocation)

Aufgabe 1
Beschreibe anhand von Beispielen, mit welchem Ziel Unternehmen Geotargeting einsetzen.

- Internationale Unternehmen setzen Geotargeting ein, um Besucherinnen und Besucher ihrer Website direkt auf die richtige Sprachversion der Seite zu leiten.
- Werbeanbieter nutzen Geotargeting, um für ihre Kunden Werbeanzeigen mit regionalem Bezug zu schalten.
- Fernsehsender nutzen Geotargeting, damit ihre Livestreams nur in ausgewählten Ländern verfügbar sind.
- Marktforscher nutzen Geotargeting, um die regionale Nachfrage nach Produkten besser einschätzen zu können.

Aufgabe 2
Hat Geotargeting (Geolocation) für die Besucherinnen und Besucher einer Website auch Vorteile?

- Websites werden direkt in der richtigen Sprache angezeigt
- beim Surfen erhält man Angebote aus der direkten Umgebung

Aufgabe 3
Auf der Website https://www.dein-ip-check.de wird unter anderem der Ort angezeigt, der aus der IP-Adresse ermittelt wird.

Welcher Ort wird für deinen Computer angezeigt?

Welche Genauigkeit wird für die Ortsangabe genannt?

Aufgabe 4
Auch Google wertet die IP-Adresse des Computers aus, wenn die Nutzerin oder der Nutzer den Standort nicht freigegeben hat.

a) Teste, ob an deinem Computer der Standort für Google freigegeben ist.
Öffne dazu Google Maps (maps.google.de).
Welchen Kartenausschnitt siehst du? Ist der Standort für Google freigegeben?

Wenn der Standort nicht freigegeben ist, wird eine Karte von Deutschland und einigen Nachbarländern angezeigt, sobald man die deutsche Seite von Google Maps öffnet (maps.google.de).

b) Gib nun in das Suchfeld „Wo bin ich“ ein. Was geschieht?

Der Kartenausschnitt wird vergrößert und zeigt im Zentrum den Ort, in dem der Computer steht.

Anonymes Surfen

Während des Surfens im Internet erzeugt man zahlreiche digitale Spuren, die erfasst, ausgewertet und zu Nutzerprofilen verknüpft werden können. Deshalb suchen immer mehr Menschen nach Möglichkeiten, im Internet ihre Privatsphäre zu schützen. Grund genug, sich mit Methoden zu befassen, die eine gewisse Anonymität im Internet versprechen.

Foto: Gerd Altmann (Pixabay)

Virtual Private Network (VPN)

Über ein Virtual Private Network (virtuelles privates Netzwerk) ist es möglich, über das Internet auf ein Netzwerk zuzugreifen, als wäre man selbst innerhalb des Netzwerks. Virtual Private Networks (VPN) werden in vielen Unternehmen genutzt, beispielsweise für Mitarbeiter im Homeoffice oder Außendienst.

Die Daten im Virtual Privat Network werden über das öffentliche Internet übertragen. VPN-Verbindungen müssen deshalb verschlüsselt sein, um die übertragenen Daten vor unbefugtem Zugriff zu schützen.

Wählt man sich in das Virtual Private Network ein, wird eine Art Tunnelverbindung ins Internet aufgebaut, die kein Außenstehender sehen kann. Dadurch ist ein Nutzer, der sich über VPN ins Internet einwählt, tatsächlich anonym im Internet unterwegs – für alle, nicht aber für den VPN-Anbieter.

Proxy-Server

Ein Proxy-Server (von englisch proxy representative „Stellvertreter“) arbeitet als eine Art Vermittlungsstelle ins Internet. Er nimmt Anfragen des Clients entgegen und leitet sie an Webserver im Internet weiter. Dabei bleibt dem Webserver die Identität des Clients verborgen.

Ein Nutzer, der sich über einen Proxy-Server mit dem Internet verbindet, genießt dadurch beim Surfen eine gewisse Anonymität. Gegenüber dem Anbieter des Proxy-Servers besteht diese Anonymität allerdings nicht, weshalb bei der Auswahl eines geeigneten Servers Vorsicht geboten ist.

Unter den Anbietern, die diese Services kostenlos anbieten, tummeln sich viele, die ihrerseits die Internetaktivitäten ihrer Nutzer auswerten und diese Daten verkaufen.

Startpage und DuckDuckGo

Startpage und DuckDuckGo sind Suchmaschinen, die keine Daten ihrer Nutzer sammeln und auswerten. Beide Suchmaschinen speichern weder IP-Adressen ihrer Nutzer noch legen sie Cookies ab.

Startpage leitet die Suchanfragen der Nutzer an die Google-Suchmaschine weiter. Da die Suchergebnisse nicht durch die IP-Adresse des Nutzers und seine vorherigen Suchanfragen beeinflusst werden, sehen alle Nutzer die gleichen, nicht personalisierten Ergebnisse.

DuckDuckGo arbeitet ähnlich wie Startpage, greift zur Ermittlung der Suchergebnisse aber auf die Microsoft-Suchmaschine Bing und weitere Quellen zurück. Dazu gehören beispielsweise vielbesuchte Webseiten wie Wikipedia.

Tor-Browser

Tor (**T**he **O**nion **R**outing, von englisch onion „Zwiebel“) ist ein Netzwerk zur Anonymisierung von Verbindungsdaten im Internet. Durch das Onion-Routing werden die Webinhalte über ständig wechselnde Routen durch das Netzwerk geleitet. Jeder dabei passierte Knoten stellt eine Art Proxy-Server dar, der die Daten ver- oder entschlüsselt. Dadurch ist die Datenübertragungsrate für Streaming o.ä. zu gering.

Der auf Mozilla Firefox basierende Tor-Browser ermöglicht aber Millionen Menschen in antidemokratischen Staaten einen unzensierten Zugang zum Internet.

Die Anonymität des Tor-Netzwerks bietet im so genannten Darknet allerdings auch Raum für Kriminelle und illegale Geschäfte jeglicher Art.

Anonymes Surfen

Aufgabe 1
Sind die folgenden Aussagen zu Verbindungen über Virtual Private Network (VPN) richtig?

▪ Eine VPN-Verbindung ist eine Art Tunnelverbindung ins Internet.	richtig
▪ Außenstehende können die Verbindung nicht sehen.	richtig
▪ Auch der VPN-Anbieter hat keinen Zugriff auf meine Daten.	falsch
▪ Die Daten im Virtual Private Network (VPN) werden über das öffentliche Internet übertragen.	richtig
▪ Eine VPN-Verbindung ist eine feste Standleitung zwischen Sender und Empfänger vertraulicher Daten.	falsch

Aufgabe 2
Beschreibe die Funktion eines Proxy-Servers bei der Verbindung ins Internet.

Ein Proxy-Server arbeitet als eine Art Vermittlungsstelle ins Internet.
Er nimmt Anfragen des Clients entgegen und leitet sie an Webserver im Internet weiter.
Dabei bleibt dem Webserver die Identität des Clients verborgen.

Aufgabe 3
Vergleiche die Suchergebnisse von Google mit den nicht personalisierten Ergebnissen von Startpage.com. Öffne nebeneinander zwei Browserfenster. Ruf in einem Fenster Google auf, im anderen www.startpage.com.

Gib nun in beiden Fenstern den Suchbegriff „Pizza" ein und vergleiche die Suchergebnisse. Was fällt dir auf?

Von den zehn Treffern auf der ersten Seite der Google-Suchergebnisse entfallen acht auf lokale Pizzerien. Erst an Platz 7 erscheint der Wikipedia-Artikel über Pizza und an Platz 10 steht ein Eintrag einer Seite mit Pizza-Rezepten.
Auf Platz 1 der Startpage-Suchergebnisse erschein der Wikipedia-Artikel über Pizza, gefolgt von der Rezeptseite, die Google an Platz 10 gelistet hat.
Danach folgen Seiten überregionaler Pizza-Lieferdienste und weitere Rezepte-Seiten.

Aufgabe 4
Welche Vor- und Nachteile bietet der Tor-Browser?

Vorteile:
- IP-Adresse wird anonymisiert
- Geoblocking lässt sich umgehen

Nachteile:
- deutlich langsamer als „normale" Browser
- Streaming nicht möglich