Editorial

Liebe Leserinnen und Leser,

ob beim Fernsehabend im heimischen Wohnzimmer, beim Surfen im Internet oder am Computer bei der Arbeit: Im Alltag werden Sie rundum beschnüffelt. Wo Anbieter kein Geld verlangen, greifen sie umso mehr Daten ab. Diesem Orwell'schen Albtraum kann man kaum entkommen, aber man kann sich zumindest über die Überwachungsmethoden informieren und allzu neugierigen Datensammlern einen Riegel vorschieben.

Dazu werfen wir in dieser Ausgabe einen Blick hinter die Kulissen. Sie erfahren, wie der Werbemarkt im Internet mit all seinen Datenbrokern funktioniert und warum Ihre Daten für diese Händler so wertvoll sind. Das kann sich auch schnell negativ auswirken, wenn Sie bei der dynamischen Preisgestaltung deutlich mehr bezahlen sollen als Ihr Nachbar.

Aber nicht nur Ihr Computer sendet Daten an die Werbeindustrie. Auch Ihr Fernseher ist neugierig, wenn er als Smart TV mit dem Internet verbunden ist. Wir erklären Ihnen, welche Werbeblocker den meisten Spam abwehren und wie Sie mit einem günstigen Raspi den unerwünschten Datenstrom filtern.

Am Arbeitsplatz ist man hierzulande noch weitgehend vor Bespitzelung durch den Arbeitgeber geschützt. Doch in den USA überwachen so viele Chefs ihre Mitarbeiter, dass sich eine ganze Industrie von dubiosen Überwachungsdienstleistern entwickelt hat: Sie protokollieren jeden Tastendruck und lesen jede E-Mail mit. Mit zunehmender Digitalisierung und Heimarbeit breitet sich dieser Trend leider auch hierzulande aus. Teilweise stiften die Programme die Mitarbeiter zur Selbstüberwachung an, um datenschutzrechtliche Einschränkungen zu umgehen. Hier hilft oft nur, sich mit anderen Betroffenen zu organisieren, wie der Soziologe Simon Schaupp im Interview erläutert.

Schließlich kann man bei ungewolltem Spam auch Schadenersatz fordern. Da sich die Datensammler immer neue Methoden einfallen lassen, muss sich auch der Datenschutz weiterentwickeln. Und bei den größten Datenfressern, den KI-Systemen und Sprachmodellen, steht die rechtliche Regulierung erst am Anfang. Mit diesem Heft geben wir Ihnen das Wissen und hilfreiche Werkzeuge an die Hand, damit Sie der übermächtig wirkenden Werbe- und Datenindustrie nicht hilflos gegenüberstehen.

Hartmut Gieselmann

Inhalt

DATEN UND GELD

Beim Surfen, beim Einkaufen und beim Bezahlen wollen Dienste Ihre Daten sammeln. Doch Sie können Datenbroker abwehren, datensparsam zahlen und in Shops sogar Geld sparen.

SCHUTZ VOR WERBUNG

Wenn Internetwerbung zu aufdringlich wird, schlägt die Stunde von Adblockern. Alternativ filtern Sie die Werbung mit dem Raspi schon heraus, bevor sie in Ihr Netzwerk fließt.

SCHUTZ VOR ÜBERWACHUNG

Ob vor der Glotze oder am Arbeitsplatz: Die einen wollen ihren TV-Konsum überwachen, die anderen ihren Arbeitsfleiß. Wir zeigen Gegenmittel und blicken auf den Unsinn anlassloser Überwachung.

DIE RECHTSLAGE

Datenschutzverstöße sind kein Spaß. In Schlaglichtern lernen Sie Ihre Rechte kennen, wie Sie diese durchsetzen und was Sündern blüht, auch auf dem relativ neuen Gebiet der KI.

ZUM HEFT

Datenlöschdienste im Internet

Jeden Tag handeln Tausende Datenbroker mit Ihren persönlichen Informationen im Internet und verdienen damit Milliarden. Das ruft Schutzdienste auf den Plan. Sie versprechen, Ihre Daten zu löschen, sodass Spammer und Betrüger Sie nicht mehr belästigen. Wir klären, was die Dienste taugen, welche Möglichkeiten Sie zusätzlich haben und wann Sie machtlos sind.

Von **Torsten Kleinz**

Bild: Thorsten Hübner

Das Angebot klingt verlockend: Sie müssen sich nie wieder selbst um widerrechtlich abgegriffene Daten kümmern, stattdessen übernehmen Dienstleister die Jagd nach E-Mail-Adressen und Telefonnummern in den Fängen von Datenhändlern. Die Hilfe ist oft nur allzu willkommen, denn als Einzelner steht man der Übermacht der Datensammler hilflos gegenüber.

In diesem Artikel untersuchen wir die Methoden und Erfolgsaussichten solcher Datenschutzdienste und geben zusätzlich Tipps, was sie selbst tun können. Auf die Hintergründe des weltweiten Geschäfts mit persönlichen Daten und die aktuelle Rechtslage in der EU und in den USA gehen wir im Artikel „Der Markt der Datenbroker“ ein.

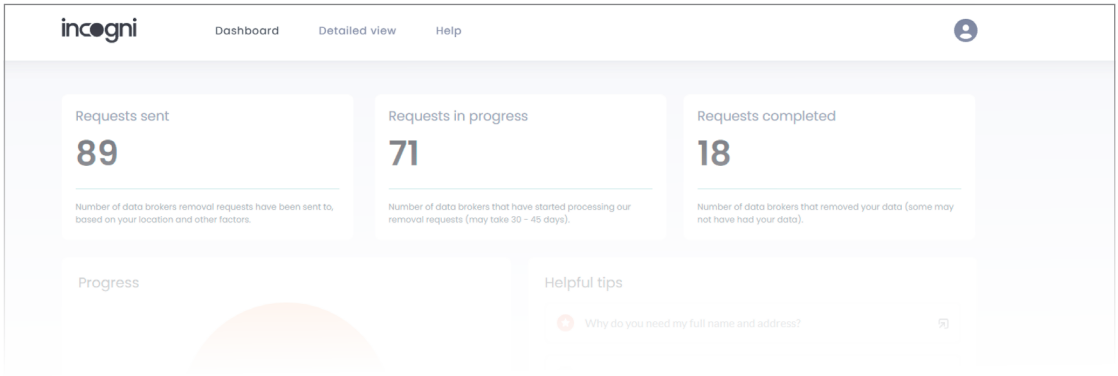
Surfshark Incogni

Seit 2021 bietet das in Litauen ansässige, aber in den Niederlanden registrierte Unternehmen Surfshark seinen Dienst Incogni an. Incogni soll E-Mail-Adressen in den Beständen von Datenbrokern aufspüren und deren Löschung fordern. Er ist einer der günstigsten Datenlöscher auf dem Markt, leistet für knapp 80 Euro im Jahr aber auch weniger als die Konkurrenz. Einen kostenlosen Probe-Account gibt es nicht, immerhin kann man bei Nichtgefallen innerhalb von 30 Tagen sein Geld zurückfordern.

Das Angebot wirkt auf den ersten Blick aufgeräumt und professionell aufgesetzt. Incogni fragt lediglich die E-Mail-Adresse sowie den Namen ab und verzichtet auf Angaben zu Telefonnummer und Adresse. Nachdem man per Kreditkarte bezahlt hat, soll man per Maus eine rechtsverbindliche Vollmacht unterschreiben, mit der Incogni die Datenlöschung bei verschiedenen Anbietern verlangt. Eine weitere Identitätsprüfung findet nicht statt.

Im Test mit einer deutschen Mailadresse landeten wir nach wenigen Minuten auf einem aufgeräumten Dashboard, das 91 Datenhändler listet. Wer will, kann sich durch die einzelnen Anbieter klicken, bekommt aber nur rudimentäre Informationen. Die Liste reicht von dem deutschen Marktforschungsunternehmen GfK über den Marketing-Anbieter ID5, der Interessenprofile für die Werbeindustrie verknüpft, bis hin zum Videoportal Dailymotion. Incogni fragte uns gar nicht erst, ob wir einen der Dienste tatsächlich nutzen, sondern verschickte sofort die Löschaufforderungen in unserem Namen.

In den folgenden Wochen konnten wir auf dem Dashboard den Fortschritt der Händlerreaktionen



Lesen Sie mehr in c’t Daten schützen 2024

Neue Spielregeln für Werbung

In den kommenden Monaten baut Google seinen Browser Chrome an mehreren Stellen um. Die Auswirkungen betreffen die gesamte Onlinewerbeindustrie, Websitebetreiber, die Entwickler von Werbeblockern und nicht zuletzt die Nutzer.

Von **Jo Bager**

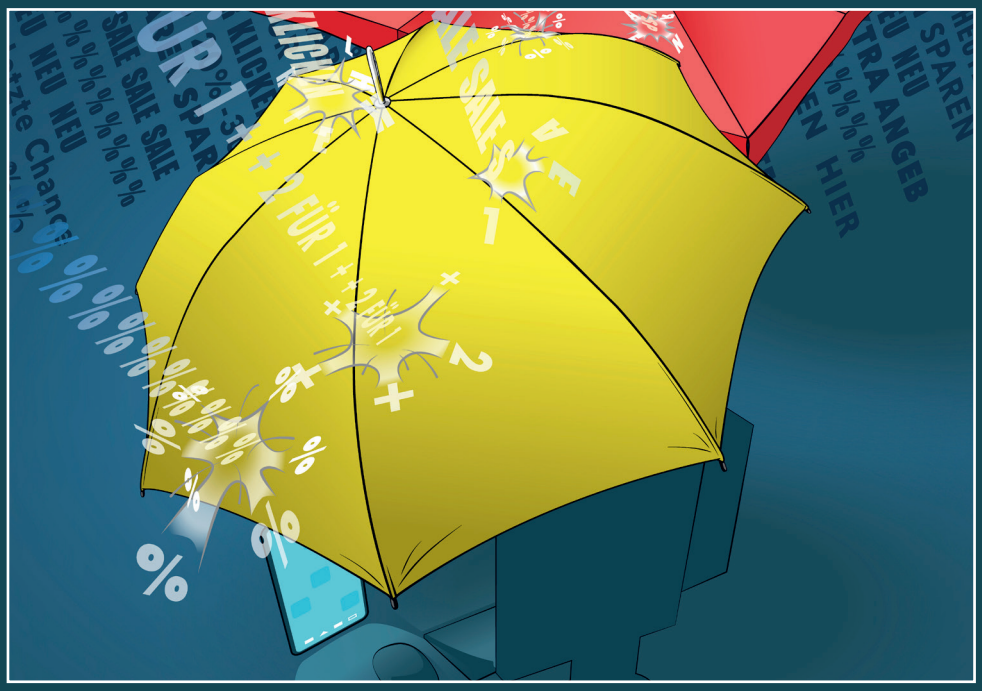


Bild: Rudolf A. Blaha

Onlinewerbung ist ein wichtiger Wirtschaftsfaktor. Hierzulande geben Unternehmen rund 5,5 Milliarden Euro pro Jahr dafür aus. Das besagen die Zahlen des Online-Vermarkterkreis (OVK) im Bundesverband der digitalen Wirtschaft.

Medien, Download-Sites, soziale Netze, Spieleplattformen: Website-Betreiber sind auf Werbung angewiesen; sie hilft, die Technik- und Personalkosten zu refinanzieren. Manches Angebot würde es ohne Werbung allenfalls nur in eingeschränkter Form geben. Und die Bedeutung der Onlinewerbung wächst weiter.

Das gilt zum Beispiel auch für die c't: Ihr Abo macht zwar den Großteil unserer Einnahmen aus; die Werbung auf unseren Webseiten trägt aber zum Umsatz bei. Nur so können wir langfristig den besten IT-Journalismus bieten.

Werbeflut nervt

Etliche Website-Betreiber übertreiben es aber mit der Werbung und überfrachten ihre Websites mit zu viel Bannern, selbst abspielenden Videos und anderen ablenkenden Inhalten. Nutzer behelfen sich dagegen mit Werbeblockern, die die störenden Elemente ausfiltern. Rund 35 Prozent der Internetnutzer haben einer Statistik des Marktforschungsunternehmens GWI zufolge im Jahr 2022 hierzulande einen Werbeblocker benutzt. Weltweit waren es knapp 36 Prozent.

Es gibt eine große Bandbreite von Werbeblockern verschiedener Bauweise. Der Artikel „12 Werbeblocker im Vergleich" vergleicht 12 Werbeblocker in puncto Blockierwirkung, Anpassbarkeit und Nutzungskomfort und zeigt, welcher Typ Werbeblocker sich für welchen Einsatzzweck eignet. Der Artikel „Starthilfe für Pi-hole und AdGuard Home" stellt die Werbeblocker Pi-hole und Adguard näher vor und gibt Tipps für deren Einrichtung.

Ware Verbraucherdaten

den Werbeplatz dazu auf einer Versteigerungsplattform: „Ich habe hier ein Skyscraper-Banner (Hochformat) für einen 50- bis 55-jährigen kaufkräftigen Mann, der sich für Autos interessiert." Auf dieses Angebot bieten dann mehrere Dienstleister, derjenige mit dem besten Angebot erhält den Zuschlag und darf seine Werbung ausspielen.

Damit solche Werbeformen funktionieren, müssen Website-Betreiber und ihre Werbepartner in großem Stil Daten über die Surfer erheben und untereinander austauschen. Typischerweise wirken dabei zwischen den werbenden Unternehmen und den Website-Betreibern etliche Dienstleister mit, die Tracking-Daten über die Website-Besucher hin- und herschieben.

Der Website-Betreiber weiß durch diese Struktur in der Regel nicht, wer bei ihm zu einem bestimmten Zeitpunkt gerade wirbt (und nebenbei Daten einsammelt) – und holt sich vom Besucher qua DSGVO-Consent-Banner die Erlaubnis für alle potenziell infrage kommenden Partner ab. Wer sich mal die Mühe macht, im Consent-Banner die Option „Werbeoptionen anpassen" oder ähnlich anzuklicken, findet nicht selten Hunderte von Unternehmen.

Neue Werbefundamente

Eine wichtige technische Grundlage für das Tracking sind die sogenannten Third Party Cookies. Damit erkennen Werbeunternehmen einzelne Nutzer bei ihren Besuchen auf verschiedenen Websites wieder und können die so gesammelten Informationen zu einem Profil zusammenfügen.

Viele Browser blockieren Third Party Cookies schon seit Langem beziehungsweise machen es Benutzern mit ihren Standardeinstellungen leicht, sie zu unterdrücken. Dazu gehören Safari, Firefox, Brave, Vivaldi und weitere. Ihre Hersteller wollen so ihre Nutzer vor Tracking schützen. Das Schwergewicht der Branche, Chrome, blockiert Third Party Cookies bisher aber noch nicht. Chrome hat weltweit einen Marktanteil von rund 65 Prozent, in Deutsch-

FAST-Spione im Smart TV

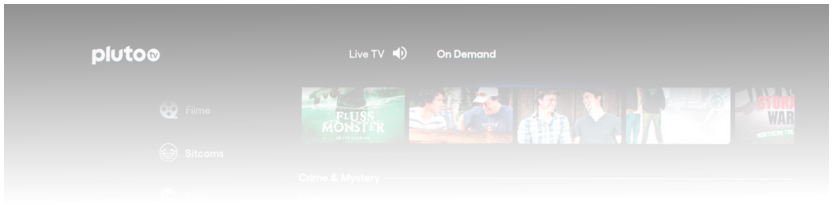
Rein werbefinanzierte Streamingdienste wollen Netflix & Co. die zahlende Kundschaft abjagen und etablierte TV-Sender ausbooten. Smart TVs spielen dabei eine tragende Rolle, denn sie sammeln die für maßgeschneiderte Werbung nötigen Nutzerdaten – also Ihre Daten.

Von **Ulrike Kuhlmann**

Wie viele Streaming-Abos haben Sie abgeschlossen? Finden sich darunter bereits kostenlose, die Werbung einblenden? In rein werbefinanzierten Videoangeboten sehen Inhalteanbieter, TV-Hersteller und Werbetreibende die goldene Zukunft. Statt linearem TV gibt es künftig lineares TV-Streaming, und statt jeden Monat teures Geld für Netflix, Disney+ oder Prime Video zu bezahlen, sollen die Zuschauer kostenlose Videostreams mit eingebauten Werbeslots abonnieren.

Auf Smart TVs sind werbefinanzierte Dienste besonders attraktiv für die Anbieter, weil vernetzte Fernseher sehr viel Persönliches über ihre Nutzer herausfinden können. Etwa den Wohnort, zu welcher Tageszeit eine Person Videos schaut und welche Inhalte sie bevorzugt. Anhand dieser Daten können Werbetreibende ein sehr genaues Nutzerprofil zeichnen, um zielgerecht Werbung einzuspielen. Wobei „Werbung“ hier nicht nur Produktfotos oder Produktclips für Marken meint, sondern auch Werbung für den nächsten Blockbuster, das kostenpflichtige Streaming-Abo oder den werbefinanzierten TV-Stream.

Laut einer Untersuchung der Marktforscher von Omdia lässt sich mit den Nutzerdaten mehr Geld verdienen als mit der schnöden Hardware: Während die TV-Hersteller mit dem Verkauf des Fernsehgeräts einmalig Erlöse erzielen, können sie das Datengold über die gesamte Nutzungsdauer von fünf bis sieben Jahren abschöpfen. Der Gewinn aus den Daten kann bis zu achtmal höher sein als durch den Geräteverkauf, erklärt Paul Grey von Omdia. So können die Hersteller ihre eigenen Produkte anhand der Nutzerdaten gezielter am Smart TV bewerben und Provisionen für eingebundene Fremdwerbung kassieren oder die Daten direkt an Werbetreibende verkaufen.



Leihen statt kaufen

Welche Blüten das treiben kann, sieht man in den USA. Dort werden Smart TVs bereits als kostenlose Leihgeräte angeboten. So schickt das Start-up Telly einen 55-Zöller als Dauerleihgabe an Nutzer, die sich im Gegenzug zu einigen Zugeständnissen verpflichten: Sie müssen den Fernseher als primäres TV-Gerät im Haushalt nutzen und ihn stets über WLAN mit dem Internet verbinden. Werbeblocker oder Modifikationen am Gerät sind verboten, die Anzahl der anwesenden Zuschauer im Raum wird per eingebauter Kamera erfasst. Außerdem müssen die Nutzer umfangreiche persönliche Angaben machen, darunter auch, welche Markenprodukte sie kaufen und wofür sie ihr Geld sonst ausgeben. Und sie müssen zustimmen, dass ihre Daten für Werbezwecke genutzt werden können, inklusive Werbe-SMS.

Das scheint erst mal absurd: Warum sollte sich jemand auf derartige Bedingungen einlassen? Allerdings bekommen die Interessenten das Gerät kostenlos und können darauf Videos und Fernsehen schauen wie auf jedem teuren Smart TV. Das dürfte nicht wenige zur Preisgabe ihrer Daten verleiten. Selbst wenn es wohl noch eine Weile dauern wird, bis hierzulande solche Leihgeräte angeboten werden: Ganz ausgeschlossen ist das nicht, wie der Blick auf die an Mindestvertragslaufzeiten geknüpften und mit nervigen Apps gespickten Smartphones nahelegt, die hiesige Kunden mit einem verbilligten Handyvertrag erhalten.

Auslaufmodell Abonnement

Kostenpflichtige Streamingdienste werden nicht nur teurer, sondern auch immer restriktiver. So verhindert Netflix die Weitergabe von Zugängen. Disney+ plant das ebenfalls [1] und will die Abo-Kosten an

EU-Regeln für DSGVO-Bußgelder

Für die europäischen Datenschutzbehörden gelten gemeinsame Grundsätze, nach denen Bußgelder zu verhängen sind. Diese lassen den Behörden in den einzelnen Ländern aber große Spielräume.

Von **Joerg Heidrich**

Bild: KI Midjourney | Collage c't

Nur nach oben sind die Grenzen gesetzlich klar geregelt: Die europäischen Datenschutzbehörden können bei Verstößen gegen die DSGVO Bußgelder in Höhe von bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens oder Konzerns verhängen. In der Praxis taten sich die Behörden der Mitgliedsstaaten in der Vergangenheit vor allem im unteren und mittleren Bereich des Spektrums schwer, angemessene und gut begründbare Bußgelder festzusetzen.

Die Folge: Die Aufsichtsbehörden agieren auch nach mehr als sechs Jahren DSGVO sehr unterschiedlich. In osteuropäischen Ländern etwa verfahren sie oft sehr milde, Bußgelder von wenigen hundert Euro auch für schwerere Verstöße von Unternehmen sind dort nicht selten. In Westeuropa wurden dagegen kaum Bußgelder unter 10.000 Euro gegen Unternehmen verhängt. Im föderalen System Deutschlands existieren sogar große Unterschiede zwischen den einzelnen Länderbehörden.

Der Europäische Datenschutzausschuss (EDSA) als Treffpunkt und Sprachrohr aller Mitgliedsstaatsbehörden hat dieses Problem erkannt und sich dessen schon vor einiger Zeit angenommen. Sein Ziel war es, einheitliche gemeinsame Richtlinien vorzugeben, an die sich alle Länder halten sollen. Ende Mai 2023 hatte man sich auf die „Guidelines 04/2022 on the calculation of administrative fines under the GDPR“ geeinigt und sie in einem 50-seitigen Dokument (ct.de/wydn) näher erläutert.

Die Leitlinien sehen ein fünfstufiges Bemessungsverfahren vor, das eine Behörde bei der Festsetzung von Geldbußen zu durchlaufen hat. Relevant sind dabei insbesondere die Art und Schwere des Verstoßes sowie der Umsatz des betroffenen Unternehmens.

1. Zunächst wird der Sachverhalt ermittelt und festgestellt, ob die einschlägigen Bußgeldvorschriften grundsätzlich anwendbar sind. Festgelegt wird auch, ob es sich bei dem Sachverhalt um einen

Meike Kamp, die Berliner Beauftragte für Datenschutz und Informationsfreiheit: „Die EDSA-Leitlinien zur Bemessung von DSGVO-Bußgeldern tragen zu einem nachvollziehbaren Verwaltungshandeln bei“.

4. Nun erst werden Höchstgrenzen für die Verstöße festgelegt, die nicht überschritten werden dürfen.
5. Im letzten Schritt wird abschließend geprüft, ob der errechnete Endbetrag den Anforderungen der DSGVO an Wirksamkeit, Abschreckung und Verhältnismäßigkeit entspricht. Die Geldbuße kann entsprechend nach oben oder unten angepasst werden, ohne jedoch die gesetzlichen Höchstgrenzen zu überschreiten. Dieser Schritt eröffnet den Behörden die Möglichkeit, das Ergebnis noch einmal individuell zu bewerten und anzupassen.

Die am Verfahren beteiligten deutschen Behörden begrüßten die Einigung und setzen sie mittlerweile auch um. Das fünfstufige Verfahren gebe klare Regeln für die Bemessung von Bußgeldern vor und trage damit zu einem nachvollziehbaren Verwaltungshandeln bei, erklärte etwa Meike Kamp, die Berliner Beauftragte für Datenschutz und Informationsfreiheit. Der damalige Bundesbeauftragte für Datenschutz Ulrich Kelber hatte die Einigung sogar als historisch bewertet, da erstmals eine Vereinheitlichung der Bußgeldpraxis in allen Mitgliedstaaten erreicht worden sei.

Allerdings ermöglicht die Neuregelung den Be-