Aktion: 1 Jahr Eset NOD32
Virenschutz Vollversion gratis

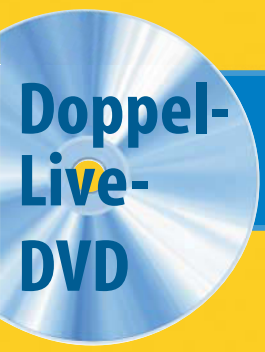
www.ctspecial.de

c't Security

c't Security

Selbst aktiv werden mit startklarer Live-DVD

Spurensuche auf Ihrem PC



Forensik mit DEFT und DART
Banking mit **c't Bankix**

Passwort-Strategie und -Tipps
Trojaner-Tricks erkennen
Cloud-Daten verschlüsseln
Datenverkehr durchleuchten
Router-Risiko zu Hause im Griff
Test Kinderschutz-Tools

Werkzeuge gegen die Datensammelwut

Werkzeugkoffer für Datensicherheit, Ihr Recht bei Behörden, Google aus dem Weg gehen, verräterische Apps finden

Doppeltes Rechenzentrum:

Dmt ncht gnz pltzlch wchtg Dtn vrschwndn.

Moderne Rechenzentren bieten eine Vielzahl von Mechanismen, um größtmögliche Datensicherheit zu gewährleisten. Aber was, wenn - etwa durch eine Naturkatastrophe, einen terroristischen Anschlag oder ein anderes unvorhergesehenes Ereignis - das gesamte Rechenzentrum ausfällt? Für viele Unternehmen wäre bereits ein 24-stündiger Ausfall der eigenen Rechenzentrums-Infrastruktur existenzbedrohend. Ein mögliches Konzept zur Vorsorge ist der Betrieb zusätzlicher Server in einem räumlich getrennten Rechenzentrum.

Darüber und über die Chancen und Möglichkeiten redundanter Rechenzentren informiert Dr. Christopher Kunz, Securityexperte bei filoo, der Hostingsparte der Thomas-Krenn.AG in seinem nächsten Webinar zum Thema „Georedundanz durch mehrere Rechenzentren".
Erfahren Sie mehr dazu unter thomas-krenn.com/redundanz

Nutzbare Sicherheit

Wenn es nach manchen Sicherheitsexperten ginge, müssten wir uns dutzende von Passwörtern aus zehn und mehr zufälligen Zeichen merken. Wer nicht schon als Kind Spaß daran fand, Telefonbücher auswendig zu lernen, fasst sich bei solchen Vorstellungen nur an den Kopf.

Mit unseren Artikeln zum Thema Sicherheit in diesem Heft gehen wir einen anderen Weg: Wir geben Anleitungen für nutzbare Sicherheit, die dem Anwender nicht im Weg stehen, sondern ihm dabei helfen, seine Aufgaben zu erledigen. So zeigen wir praktische Verfahren, das Passwort-Chaos zu meistern. Wir bieten Ihnen mit dem c't-Bankix ein wirklich sicheres und trotzdem einfach zu nutzendes System fürs Online-Banking. Und wir zeigen, wie Sie den immer häufiger auftretenden Sicherheitsproblemen in Routern aus dem Weg gehen.

Wenn Sie beim Thema Sicherheit jedoch eher die Neugier antreibt, dann empfehle ich Ihnen unseren Schwerpunkt zum Thema Forensik ab Seite 32. Dort zeigen Profis ganz praktisch und zum selber Nachmachen, welche Spuren man auf einem Windows-PC zu Tage fördern kann. Sie werden erstaunt sein, was Sie da alles finden.

Jürgen Schmidt

Inhalt

Datengier

6 Was Android-Geräte nach Hause funken

10 Nutzer-Tracking mit Fingerprints

14 Netzmacht Google

20 Wie Google-Werkzeuge auf fremden Websites Daten sammeln

24 Erfahrungen mit dem Datenschutz in der Behördenpraxis

28 Datenauskünfte von Unternehmen und Behörden einholen

Kontrolle über die eigenen Daten

32 Forensische Analyse eines PC mit DEFT

38 Forensik-Tools für Windows

42 Das verrät Ihr PC: Spurensuche auf der Festplatte

47 Wer ist „Miriam"?

48 Kali Linux: Sicherheit testen, Netzwerk durchleuchten, Daten retten

52 E-Mails sicher archivieren

54 Betrügerische Mails erkennen

58 Google aus dem Weg gehen

64 Die Anti-Antivirus-Tricks der Trojaner

70 Smartphone-Ortung verhindern

Passwort

72 Ein neues Konzept für den Umgang mit Passwörtern

76 Werkzeuge gegen das Passwort-Chaos

82 Kennwörter mit Zettel und Stift verwalten

Router

86 Router-Angriffe erkennen und abwehren

90 Updates für Ihren Router

94 Angriffen auf Router vorbeugen

Tools für mehr Schutz und Aufklärung

32 Forensische Analyse eines PC mit DEFT

38 Forensik-Tools für Windows

118 Kinderschutz-Software für Windows

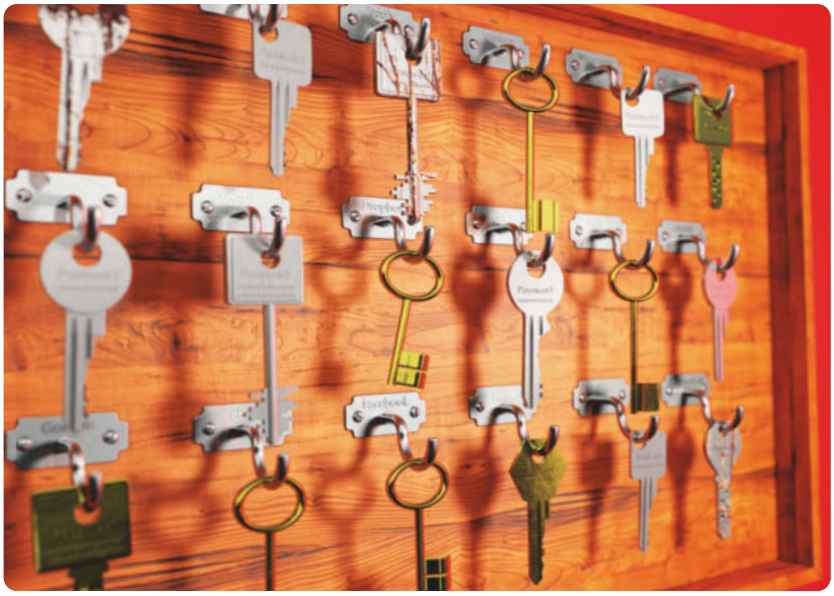
162 Sicheres Online-Banking mit c't Bankix

Tools und Know-how gegen die Datensammelwut

6 Was Android-Geräte nach Hause funken

20 Wie Google-Werkzeuge auf fremden Websites Daten sammeln

28 Datenauskünfte von Unternehmen und Behörden einholen



Passwort-Strategie und -Tipps

72 Ein neues Konzept für den Umgang mit Passwörtern
76 Werkzeuge gegen das Passwort-Chaos
82 Kennwörter mit Zettel und Stift verwalten

Kinderschutz im Internet

114 Gefahren unter Windows, Android und iOS abwehren
118 Kinderschutz-Software für Windows
124 Filternde Browser für Android, iOS und Windows Phone
128 Wie Sie Ihren Gerätepark kindersicher machen

96 Wie Sie einen unsicheren Router schnell ersetzen
100 Alt-PC zum Router umrüsten
104 Datendiebe auf frischer Tat ertappen
108 Maulkorb für Datenspione

Sicher im Netz

114 Gefahren unter Windows, Android und iOS abwehren
118 Kinderschutz-Software für Windows
124 Filternde Browser für Android, iOS und Windows Phone
128 Wie Sie Ihren Gerätepark kindersicher machen
132 DANE schützt Mail
136 DNSSEC und DANE auf Linux-Servern konfigurieren
140 DNSSEC für Clients und Netze
142 Gefahren der Tor-Nutzung im Alltag
144 Die Schwächen der E-Mail und was dagegen hilft
148 Sichere Kurznachrichten – mehr als verschlüsseln
151 Webmail abhörsicher
152 Daten im Cloud-Speicher verschlüsseln
158 Stand der Dinge im NSA-Skandal
162 Sicheres Online-Banking mit c't Bankix
166 Privatspäre sichern per VPN

Zum Heft

3 Editorial
85 Aktion NOD32 Antivirus 7
157 Impressum
157 Inserentenverzeichnis

Achim Barczok

Was Android-Geräte nach Hause funken

Zwar positionieren Hersteller ihre Smartphones gerne als Datentresore, die private Nachrichten, Adressbücher und Ortsdaten sicher verwahren. Doch tatsächlich steht die Tür offen – still und heimlich greifen Apps und persönliche Dienste Daten ab.

Wissen Sie, was Ihr Smartphone über Sie verrät? Hier drei Beispiele, die selbst die pessimistischsten Security-Experten in der c't-Redaktion überrascht haben: Die Musik-App Shazam sammelt Ortungsdaten und übergibt sie an Werbepartner. Das Spiel „Wer wird Millionär? 2014“ spioniert aus, welche Apps der Nutzer sonst noch installiert hat – ohne dass man überhaupt weiß, dass das Spiel auf diese Informationen zugreifen darf. Sonys Fernlöschdienst MyXperia merkt sich Telefonnummern und die letzte Position von Handys, selbst wenn man den Dienst nie aktiviert hat.

Um die Datengier von Android-Smartphones und -Tablets zu überprüfen, haben wir Geräte verschiedener Hersteller und rund 50 kostenlose Apps daraufhin überprüft, welche Daten sie im Hintergrund versenden. Dazu haben wir uns zwischen Smartphone und Internet geklemmt und sowohl die offene (HTTP) als auch die verschlüsselte (HTTPS) Kommunikation abgehört. Auf diesen Weg bekommt man zwar nicht alles mit: Einige Apps lassen sich so nicht austricksen, etwa weil sie andere Kanäle nutzen. Aber schon das Ergebnis dieser Auswertung lässt aufhorchen: Fast alle Apps senden systematisch Details wie Kennnummern und Geräte-Infos an Werbepartner und Statistikunternehmen. Vereinzelt speichern sie auch Adressbücher, Ortsdaten und Netzwerkinformationen. An dieser heimlichen Datensammelei beteiligen sich selbst Gerätehersteller und der Android-Entwickler Google.

Androids Rechtesystem

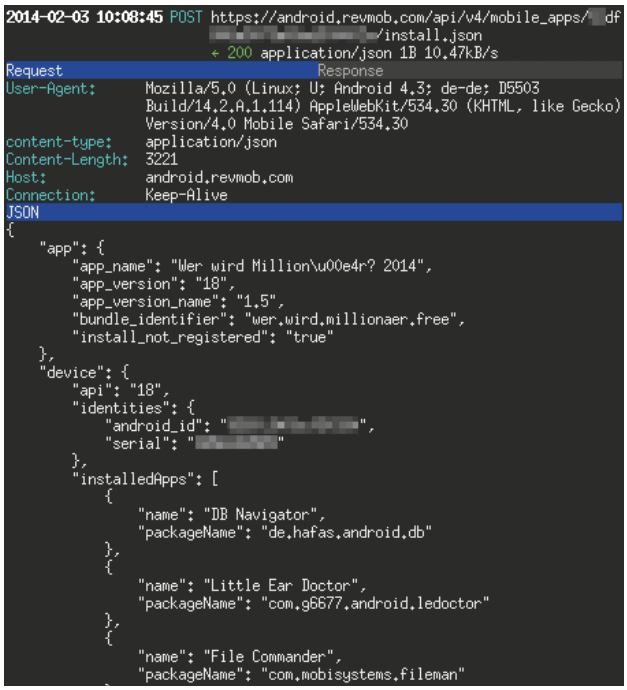
Hauptursache für die Datenlecks ist das undurchsichtige Rechtesystem für Android-Apps. Während der Installation einer App muss man ihr grundsätzlich alle Rechte gewähren, die sie im Laufe der Nutzung möglicherweise brauchen könnte. Bietet ein Dienst beispielsweise eine ortsbasierte Suche an, muss man ihm selbst dann den Zugriff auf die Smartphone-Position geben, wenn man diese Funktion nie nutzen möchte. Nimmt sich die App außerdem das Recht, auf das Internet zuzugreifen, kann sie Daten heimlich nach Hause oder an den Server eines Werbepartners senden. Dazu kommt eine uneinheitliche und oft unzureichende Informationspolitik der App-Hersteller.

Die gesammelten Daten können sich deshalb zu einem ausführlichen Nutzerprofil zusammenfügen, weil jede App auf die weltweit einzigartige Android-ID des Smartphones zugreifen darf. App-Entwickler und Werbepartner können so Datensätze aus unterschiedlichen Quellen zu einem Nutzerprofil verknüpfen. Im Prinzip funktioniert die Android-ID ähnlich wie ein Browser-Cookie, nur dass man sie nicht ohne Weiteres löschen kann. Erst wenn man das Smartphone komplett zurücksetzt, erzeugt es eine neue ID.

Aufgrund der datenschutztechnischen Problematik einer solchen eindeutigen Identifikationsnummer hat Apple vor einiger Zeit für sein Betriebssystem iOS eine Werbe-ID eingeführt, die der Anwender jederzeit zurücksetzen kann. Google hat für Android ein vergleichbares ID-System entwickelt und schreibt Entwicklern seit August 2014 vor, zu Werbezwecken nur noch diese zu verwenden. Viele halten sich aber nicht daran.

Datensammler

Dass manche Apps mehr dürfen als andere, ist vom Nutzer prinzipiell gewollt: Schließlich möchte man ja vielleicht, dass Google Maps mit Hilfe der eigenen Position eine Übersichtskarte liefert oder dass man ohne lästiges Abtippen der Namen alle Freunde in einem sozialen Netzwerk findet. Der Ortsdienst Foursquare beispielsweise kann auf Wunsch das Smartphone-Adressbuch mit den Foursquare-Servern abgleichen, um Kontakte zu finden. Nur muss man der App dieses Recht auch einräumen, wenn man die Funktion gar nicht braucht. Immerhin fragt Foursquare den Nutzer, ob man seine Kontakte mit Foursquare abgleichen will. Allerdings dürfte nicht jedem dabei klar sein, dass ein Tipp auf die Einstellung „Finde Freunde aus deinem Adressbuch“ sämtliche E-Mail-



Revmob, der Werbepartner des beliebten Spiels „Wer wird Millionär? 2014“, fragt heimlich die Liste aller installierten Apps ab.

Adressen und Telefonnummern auf den Foursquare-Server hochlädt. Die Messaging-Dienste Whatsapp und Viber verschicken die Telefonnummern automatisch, nachdem man die Geschäftsbedingungen beim ersten Start angenommen hat. Informationen über diesen Datenaustausch stehen nur im Kleingedruckten der Datenschutzbedingungen.

Warum der Musik-Erkennungsdienst Shazam die genaue Position des Smartphones erfasst, erschließt sich erst beim Lesen der Datenschutzrichtlinien. Die App bietet eine Funktion an, zu jedem erkannten Lied auch zu speichern, wo man es gehört hat. Daran dürften die wenigsten Anwender interessiert sein, trotzdem ist die Funktion standardmäßig aktiviert und muss per Opt-Out in den Einstellungen abgeschaltet werden. Was der Nutzer nicht erfährt: Ermittelte Ortsdaten gibt Shazam gleichzeitig an seinen Werbepartner AppNexus weiter, der sie inklusive einer aus der Android-ID erzeugten Kennziffer überträgt. Besonders perfide: Selbst wenn man das ortsbasierte Taggen deaktiviert hat, fließen diese Daten weiter stillschweigend an die Werbepartner.

Auch die Datengier des Spiele-Anbieters Zynga ist schlecht nachvollziehbar: Zur Identifizierung des Nutzers benutzt er inzwischen zwar die Werbe-ID, überträgt aber auch die einzigartige Gerätekennung IMEI (International Mobile Equipment Identity), die selbst beim Zurücksetzen eines Smartphones bestehen bleibt. Dazu kommen die eindeutig identifizierbare MAC-Adresse der WLAN-Schnittstelle, der Provider und Smartphone-Details wie der Gerätetyp, die Android-Version und die Auflösung. Diese Daten sammelt Zynga in Spielen wie „Words With Friends“ oder „Zynga Poker“.

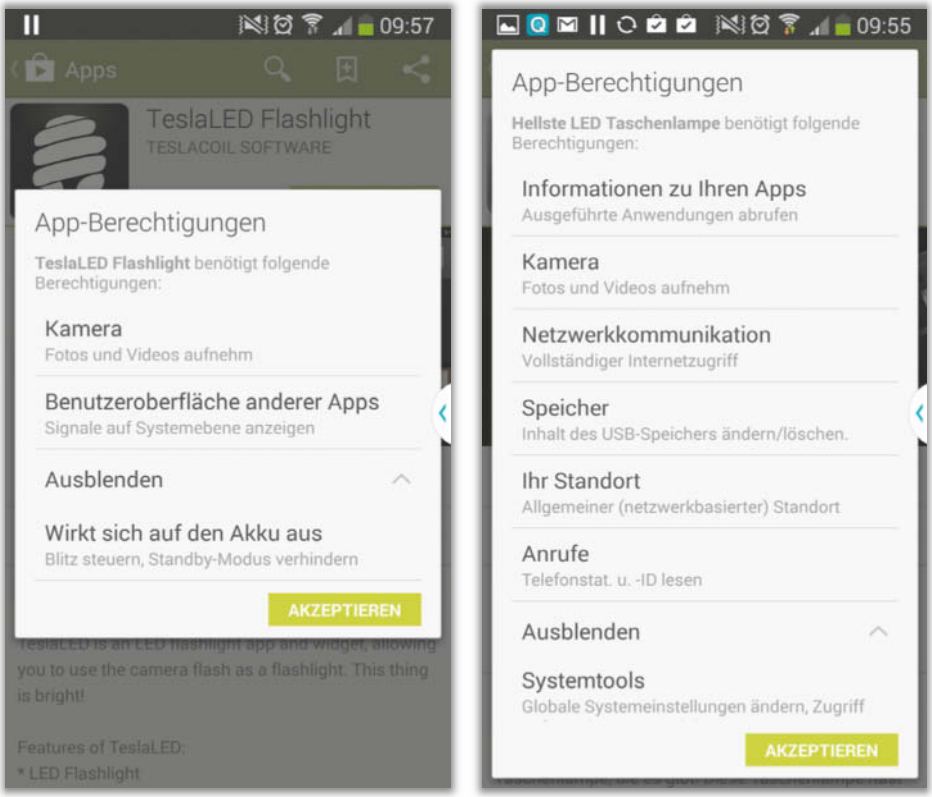
Je mehr die Werbenetze über den Nutzer wissen, desto mehr können sie an ihm verdienen. Das Spiel „Subway Surfer“ von Kiloo beliefert gleich mehrere Werber und verrät einigen davon MAC-Adresse, Seriennummer, den Namen des Mobilfunk-Providers und des WLAN.

Die App „Wer wird Millionär? 2014“ kooperiert mit dem Werbenetzwerk Revmob. Dieses greift gemeinsam mit der Android-ID auch eine Liste aller installierten Apps des Smartphones ab. Datenschutzrichtlinien hat der Anbieter des Spiels nicht veröffentlicht. Selbst die Android-Berechtigungen der App geben keinen Hinweis darauf, dass ein solcher Datenzugriff stattfindet. Beim Nachfolger „Wer wird Millionär? 2015“ tritt das Vorhalten nicht auf.

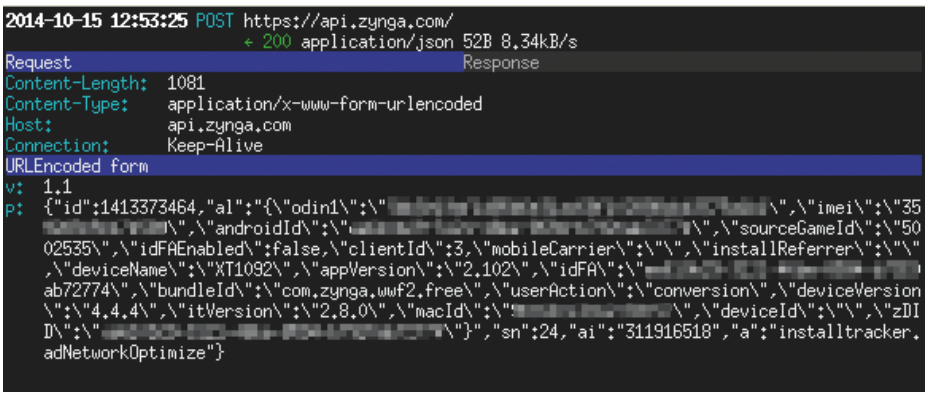
Statistik und Analyse

Viele App-Entwickler arbeiten mit Analyse-Unternehmen zusammen, die ihnen wertvolle Statistiken zur Nutzung liefern können. Der beliebteste heißt Flurry und wird beispielsweise von Quizduell, Skype und DB Navigator verwendet. Diese Apps senden unter anderem die Android-ID und Gerätedetails zum Anbieter. Einige App-Hersteller übergeben auch mehr: Skype und die LED-Taschenlampe von iHandy senden die Nutzungsdauer der Apps. Mit Hilfe der Android-ID kann Flurry theoretisch ein App-übergreifendes Profil des Anwenders erstellen. Auf seiner Webseite gibt Flurry detailliert Auskunft, welche Daten es allgemein sammelt. Verborgen bleibt jedoch, von welchen Apps das Unternehmen welche Daten bekommt.

Deutlich besser macht es die IVW (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern), über die fast alle großen Webseitenbetreiber in Deutschland ihre Inhalte erfassen. Mit Hilfe dieser statistischen Kennwerte berechnen Verlage die



Die Taschenlampen-App „TeslaLED Flashlight“ (links) holt sich nur die Rechte ein, die sie wirklich braucht. „Hellste LED Taschenlampe“ (rechts) will auch Zugriff auf vertrauliche Informationen.



Das Spielenetzwerk Zynga sammelt allerlei sensible Daten des Nutzers.

Reichweite ihrer Produkte, um Preise für Anzeigen festzulegen. Sie sammelt inzwischen nur noch die Android-ID und die ID der App-Installation und übergibt sie als MD5-Hash, sodass sie nicht so leicht einer Person zuzuordnen ist. Jede App, die mit der IVW zusammenarbeitet, muss einen Schalter zum Deaktivieren der Datensammelei einbauen.

Google, Samsung und Co.

Selbst ohne Zusatz-Apps kommunizieren Smartphones mit dem Netz, ohne dass der Anwender etwas davon mitbekommt. Der Großteil dieses Datenaustauschs zwischen Gerät und Hersteller ist eher harmlos und dient dem Nutzer. Ein Google-Telefon fordert im Hintergrund anonym die neuesten Almanach-Daten für eine schnellere GPS-Ortung an, sucht nach Updates, aktualisiert Wörterbücher für die Tastatur und lädt Blacklists für bekannte SMS-Schädlinge und Handbücher für Smartphone-Funktionen herunter. Dabei werden bestenfalls die Modell-Bezeichnungen oder Landes-Codes übertragen.

Hat man ein Google-Konto eingerichtet, fließen auch vertrauliche Infos. Kontakte, Termine, Fotos und dergleichen synchronisiert Google automatisch, wenn man deren Abgleich vorher nicht explizit deaktiviert hat. Unter den Einstellungen kann man genau festlegen, was abgeglichen wird. Google verwendet die Android-ID, Gerätehersteller wie HTC, Samsung oder ZTE überprüfen für Registrierungsvorgänge und Dienste auch die IMEI-Nummer.

Einige vorinstallierte Dienste verknüpfen diese eindeutige Nummer mit privaten Daten. Hat man beispielsweise den Geschäftsbedingungen des Samsung-Chatdienstes Chat On zugestimmt, erhält der Hersteller sofort die IMEI, die eindeutige Kennnummer der SIM-Karte und die Telefonnummer. Der vorinstallierte Sprachdienst von Samsung schickt alle Namen aus dem Adressbuch zu Samsung – um die Spracherkennung zu verbessern. Der Nutzer erfährt die mögliche Übertragung solcher Daten nur, wenn er die Details der Geschäftsbedingungen der Dienste durchliest.

Am wissbegierigsten ist aber Sony. Über dessen Dienst MyXperia kann man sein Smartphone aus der Ferne orten und löschen. Dafür übertrug Sony auf unserem Test-Smartphone Xperia Z1 Compact bei jedem Starten des Telefons die genaue Position, die Kennnummer der eingelegten SIM-Karte samt Telefonnummer und diverse Hardware-Infos wie den Batteriestatus und den aktuellen SD-Speicherplatz – ohne dass wir den Dienst aktiviert hatten.

Abhilfe

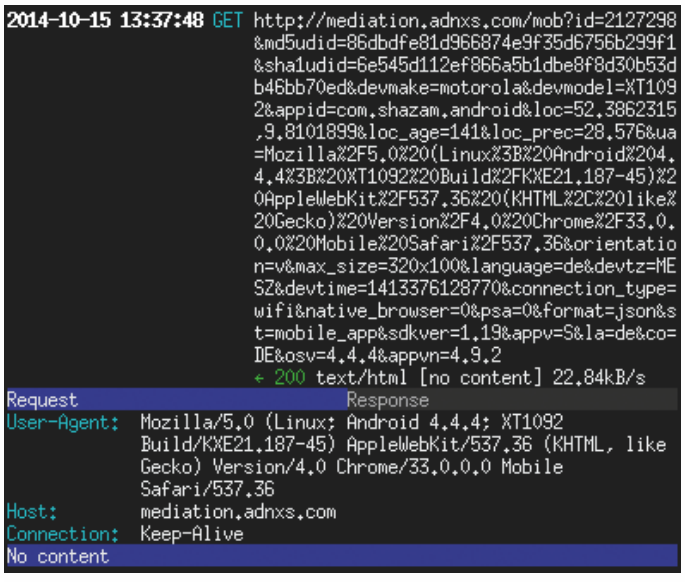
App-Anbieter, Werbenetzwerke, Smartphone-Hersteller, Google: Alle schöpfen die vertraulichen Daten der Nutzer ab und informieren darüber meist nur im Kleingedruckten ihrer Datenschutzrichtlinien. Ein einzelner Datenschnipsel gibt zwar meist nur kleine Details aus dem Leben des Nutzers preis. Doch in einer Welt vernetzter Werbenetzwerke und Geheimdienste, die Apps ausspionieren, lassen sich solche Daten schnell zu einem aussagekräftigen Puzzle zusammenfügen. Die allzu schnelle Weitergabe eindeutiger Kennzeichen wie Android-ID oder IMEI macht dies sogar sehr leicht.

Komplett abstellen kann man die Sammelei nicht: Solange das Gerät mit dem Internet verbunden ist, sendet es auch Daten. Verhindern kann man immerhin die Weitergabe der genauen Position des Smartphones über „Einstellungen/Standortdienste“. Dann funktionieren allerdings auch Navi-Apps und ortsbezogene Dienste nicht mehr, weil Android nur zwei globale Schalter bereitstellt: einen für alle Google-Apps, einen für alle anderen. Unter Android 4.3 lassen sich bestimmten Apps einzelne Rechte über ein verstecktes Menü entziehen; das alternative Android-ROM Cyanogenmod bietet diese Funktion seit Version 10.1 von Haus aus an.

Einen Teil des Datenverkehrs kann man aber auch ohne Einschränkung der App-Rechte unterbinden, indem man einen Ad-Blocker wie AdAway auf dem Smartphone installiert und die Hostnamen bekannter Übeltäter blockiert. Dazu muss das Smartphone gerootet sein, weil die Werbeblocker sonst nur in WLANs funktionieren und nicht über Mobilfunk. Eine Liste der uns bekannten Werbenetzwerke stellen wir Ihnen über den c’t-Link bereit.

Oft hilft aber auch schon, bei der Installation einer App ein genaues Auge auf die Liste der angeforderten Systemrechte zu werfen: Will eine Taschenlampen-App mehr als den Zugriff auf die Kamera und deren LED, hat sie auf dem Smartphone nichts zu suchen. (acb)

www.ct.de/cs1404006



Shazam gibt Ortsdaten an Werbepartner weiter. Übertragen werden sie über die angefragte URL. ct

GERMAN# SICHERHEIT

IT IS NOT SAFE UNTIL IT'S SICHER.

JETZT AUF GDATA.DE

Ihr Leben findet online statt. Die Sicherheit Ihrer persönlichen Daten sollten Sie dabei einem erfahrenen Profi anvertrauen. Wir bei G DATA forschen bereits seit mehr als 25 Jahren an immer neuen Lösungen für Ihre IT-Sicherheit.

Streng nach deutschen Datenschutzgesetzen und Qualitätsstandards. Mit Erfolg: Sieben Mal in Folge hat uns die Stiftung Warentest den besten Virenschutz attestiert.

Das ist GERMAN SICHERHEIT.

G DATA | TRUST IN GERMAN SICHERHEIT

GDRANZ DE INSUS Box 10-2014 210x297 • 0410090104

Herbert Braun, Frank Puscher

Nutzer-Tracking mit Fingerprints

Raffiniert, versteckt und kaum zu verhindern sind die neuen Tracking-Methoden, mit denen Werbeunternehmen überall im Web Surfer verfolgen. Browser-, Canvas- und Clock-Skew-Fingerprinting werfen viele Fragen auf – nicht nur technischer Natur.

Weite Teile der Netzöffentlichkeit schreckten auf, als Forscher der Universitäten Princeton und Leuven ihre Feldstudie über moderne Tracking-Techniken veröffentlichten [1]. Die Mitte 2014 bekannt gewordene Studie untersucht die Technik und Verbreitung von drei unterschiedlichen Verfahren: Evercookies, die sich durch verschiedene Speichertechniken von selbst regenerieren können, Cookie-Synchronisation, bei der Werbenetzwerke ihre Daten untereinander austauschen, und Canvas-Fingerprinting.

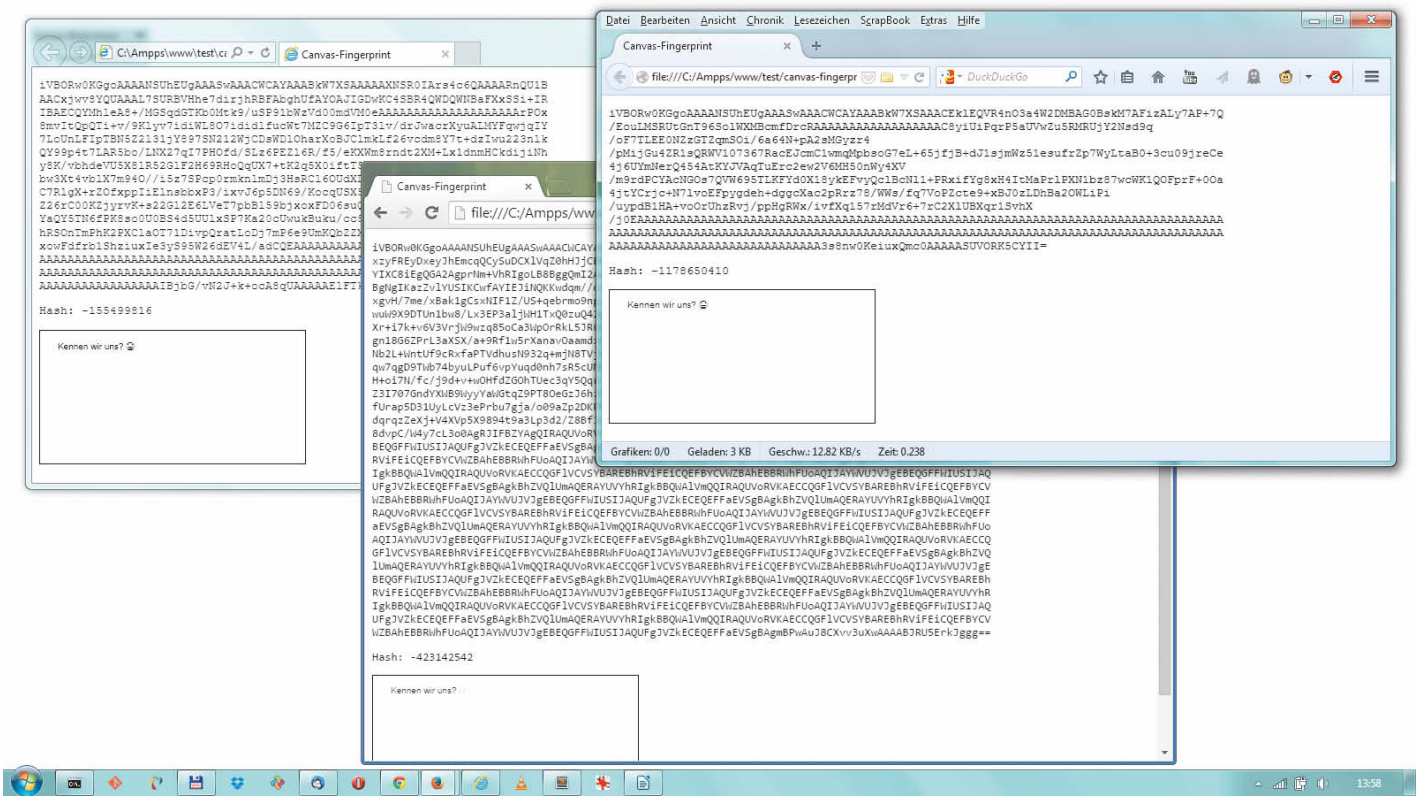
Besonders letzteres sorgte für Aufsehen, denn bislang hatte kaum jemand von diesem Verfahren gehört – dabei setzen es bereits mehr als 5 Prozent der laut Alexa-Ranking führenden 100 000 Websites ein. Das Funktionsprinzip ist gleichermaßen raffiniert und überraschend.

Canvas ist ein Verfahren, um mit JavaScript zu zeichnen. Eine Seite kann ein Canvas-Element enthalten, in dem JavaScript-Befehle einfache Formen, Farben, Schriften und Bilder zu einer Pixelgrafik anordnen. Durch schnellen Austausch dieser Grafiken entstehen Animationen; eines der wichtigsten Einsatzgebiete sind Browser-Spiele.

Auch kann die Seite Anweisungen in der Sprache WebGL an den Browser übergeben, welche dieser ohne Umweg über den Hauptprozessor an die Grafikkarte weiterleitet. Auf diese Weise kann eine Webseite aufwendige 3D-Grafiken darstellen – wenngleich WebGL nicht von allen Geräten und Browsern unterstützt wird: Internet Explorer und die iOS-Variante von Safari kennen diese Technik erst in der jeweils jüngsten Browser-Version.

Abweichung

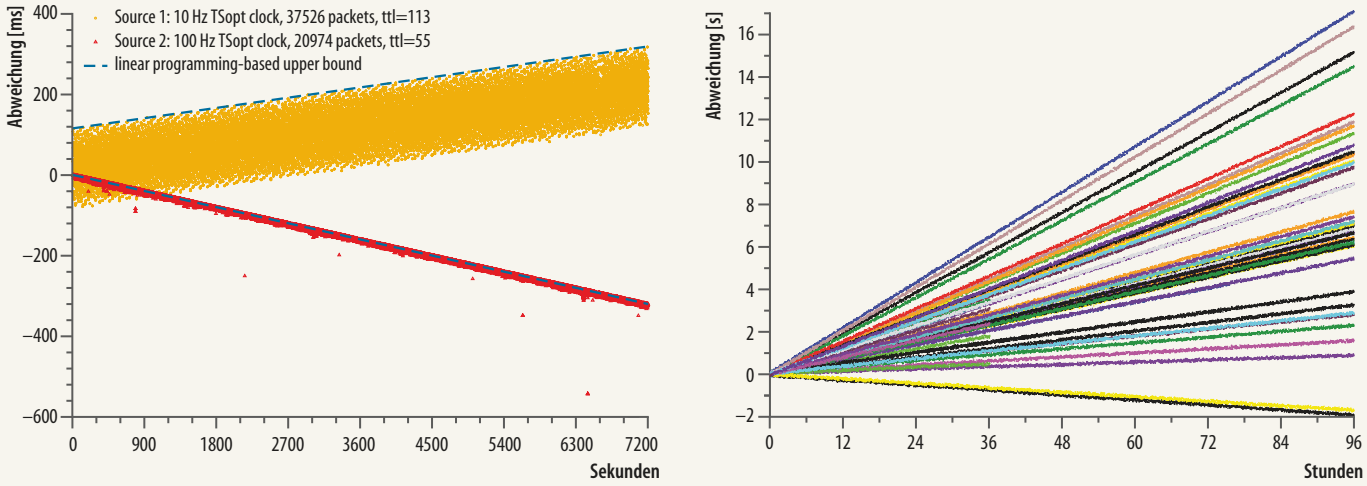
Die per Canvas erzeugte Pixelgrafik kann der Browser in Formate wie JPEG oder PNG umwandeln. Bei gleichem Input produzieren alle Browser das gleiche Ergebnis – sollte man meinen. Doch im Juni 2012 stellten Keaton Mowery und Hovav Shacham, zwei Forscher an der Universität im kalifornischen San Diego, überraschend fest, dass mit Can-



Die von Internet Explorer (links), Firefox (rechts) und Chrome (unten) generierten Bilder sind mit bloßem Auge nicht unterscheidbar – doch der Bild-Quelltext offenbart Unterschiede.

Individuelle Abweichungen

Die im TCP-Timestamp vorhandenen Abweichungen von tatsächlichen Paket-Sendeabständen ergeben über die Zeiten einen Balken (links). Bereinigt zu Linien lassen sich für verschiedene Geräte jeweils individuelle Steigungen ermitteln, anhand derer die Hardware wiedererkannt werden kann.



vas erzeugte Grafiken oft winzige Unterschiede aufweisen [2].

Offenbar führen Unterschiede der Browser beim Rendering von Texten und Grafiken sowie kleine Optimierungen der Grafikkarten bei der Ausführung von WebGL dazu, dass dieselbe Canvas-Grafik auf unterschiedlichen Systemen unterschiedlich aussieht. Am einfachsten lässt sich dieser Effekt nachvollziehen, wenn man Schrift rendert, wie wir es für den Screenshot links unten gemacht haben:

```
var canvas = document.createElement?
 ("canvas");
var context = canvas.getContext("2d");
context.fillText("Kennen wir uns?", 20, 20);
var dataURL = canvas.toDataURL?
 ("image/png");
```

Es ist nicht einmal nötig, dass der Browser das canvas ins HTML-Gerüst einbaut. Im gerenderten Bild lassen sich die Ergebnisse in Firefox, Internet Explorer und Chrome optisch kaum auseinanderhalten. Gibt man es jedoch als Daten-URL (also als Base64-kodierten String) aus, ist der Unterschied offensichtlich. Bereits mit diesem einfachen Versuchsaufbau ergaben sich 50 verschiedene Ergebnisse.

Kompakt zusammenfassen lässt sich das Ergebnis mit einer Hash-Funktion, die ebenfalls nur wenige Zeilen erfordert und zum Beispiel eine kurze Zahl auswirft. Rendert ein Browser dasselbe Bild auf demselben Gerät wiederholt, entsteht wieder derselbe Hash-Wert.

Der Entwickler Valentin Vasilyev knüpfte an die Arbeit der beiden Forscher an und programmierte ein unter Open-Source-Lizenz veröffentlichtes Fingerprinting-Skript. Er konnte es auf einer Website mit Millionen von bereits identifizierten Nutzern ausprobieren und somit die Ergebnisse deutlich verbessern: Nach eigenen Aussagen lieferten 89 Prozent der getesteten Browser eindeutige Fingerabdrücke.

Dabei benutzte Vasilyev nicht nur Canvas-Fingerprinting (schattierter Text und ein farbiges Rechteck), sondern ließ auch die Ergebnisse der Aussagen des Browsers über sich selbst einfließen – Browser-Kennung, Plug-ins, Sprache, Farbtiefe und Zeitzone. Das Skript generiert die Grafik, extrahiert die Daten-URL, wirft diese mit den Browser-Daten zusammen und errechnet daraus den Hash-Wert.

Vasilyevs Auftraggeber war nicht zufrieden mit der Erkennungsrate, vor allem bei Mobilgeräten, und brach die Versuche ab. Doch andere Unternehmen sammelten Erfahrungen und Daten mit seinem Skript. Beispielsweise testete es das zum Verlag Gruner und Jahr gehörende Werbenetzwerk Ligatus; mittlerweile hat Ligatus den Test nach eigenen Angaben beendet. Andere versuchten, es weiter zu optimieren. Ein unter einer vietnamesischen Domain gehostetes Skript etwa probiert 1126 Fonts durch.

Schnüffel-Widget

Laut der eingangs erwähnten Feldstudie setzen 5559 Websites bereits Canvas-Fingerprinting ein. Die überwiegende Mehrheit der betroffenen Websites nutzt ein Widget von AddThis. Es zeichnet den alle lateinischen Buchstaben enthaltenden Text „Cwm fjordbank glyphs vext quiz“ sowie ein Rechteck auf die Leinwand, die per CSS unsichtbar gemacht wurde; nach dem Extrahieren des Fingerprints zerstört das Skript das Canvas.

Man darf annehmen, dass die meisten Website-Betreiber nicht wissen, was sie sich da eingehandelt haben. Denn nur ein kleiner Teil des unkomprimiert mehr als 10 000 Zeilen langen AddThis-Skripts beschäftigt sich mit Tracking. Der Dienst ist bekannt dafür, Webseiten mit Widgets zu versorgen, über die sie Sharing-Buttons für Facebook, Twitter et cetera anbieten können – doch dabei füllt AddThis auch die eigenen Datenbanken.

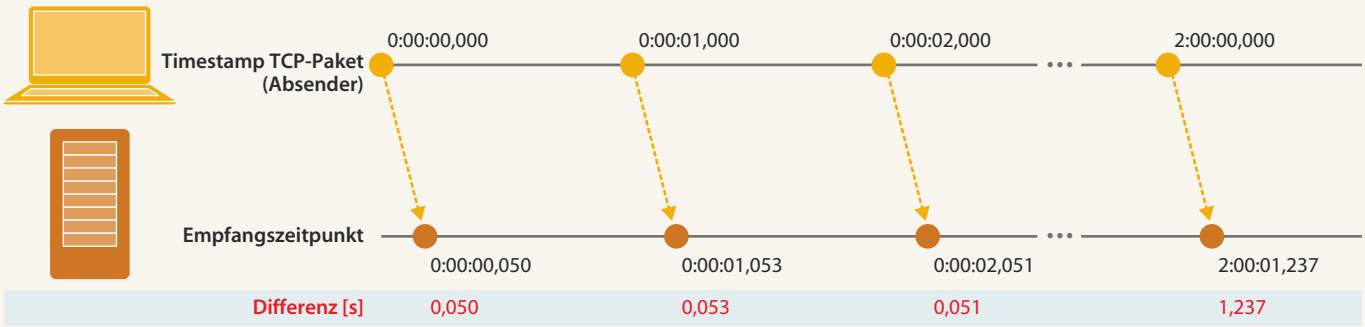
Die in Mobilgeräten vorinstallierten Browser dürften sich per Fingerabdruck schwer identifizieren lassen – zu standardisiert sind dort Hard- und Software. Bei Desktop-Rechnern sind technische Maßnahmen gegen das Canvas-Fingerprinting schwierig. Das Abschalten von JavaScript oder extern nachgeladenen Skripten hilft, schränkt aber die Praxistauglichkeit für den Anwender ein. Der „Privacy Badger“, eine Browser-Erweiterung der Verbraucherschutzorganisation Electronic Frontier Foundation, soll in einer künftigen Version Browser-Fingerprinting unterbinden. Mowery und Shacham schlagen Browser-Herstellern vor, canvas.toDataURL() nur nach Bestätigung durch den Anwender auszuführen.

Taktabweichung

Letztlich ist Canvas-Fingerprinting nur eine weitere von vielen Methoden zum Tracken individueller Nutzer. Eine gar nicht so neue

TCP-Timestamp-Differenzen

Über längere Zeit summiert sich die Differenz zwischen TCP-Timestamp und Empfangszeitpunkt auf unterscheidbare Werte.



Technik erregt erst seit Kurzem die Aufmerksamkeit vieler Werbefirmen und wird in ihren Software-Analyselabors so ausgiebig wie konspirativ getestet. Auch beim sogenannten Clock-Skew-Fingerprinting geht es darum, den Nutzer-Client eindeutig zu identifizieren. Das System wurde bereits 2005 von der Universität San Diego und dem kooperierenden Forschungsinstitut CAIDA vorgestellt und erobert sich wohl bald einen festen Platz im Werkzeugkasten der Tracking-Anbieter.

„Clock Skew" bedeutet in etwa „Taktabweichung". Der Begriff beschreibt minimale Drifts eines jeden Taktgebers in PCs oder auch Smartphones. Diese Drifts resultieren aus Fertigungsdifferenzen, etwa Unreinheiten in den verwendeten Quarzen oder unterschiedlich langen Leiterbahnen. Längst sind Security-Techniker auf die Idee gekommen, sich diese Differenzen zunutze zu machen, um Geräte zu identifizieren.

Damit ein Webserver den Clock Skew des Clients messen kann, muss er an dessen Zeiterfassungsdaten kommen. Die CAIDA-Forscher aus San Diego um den Doktoranden Tadayoshi Kohno machten sich zunutze, dass Geräte meist von der per RFC definierten Option Gebrauch machen, jedes gesendete TCP-Paket mit einem Zeitstempel zu versehen (TCP Timestamp, RFC 1323). Als Zeitgeber für die Stempel fungiert hier in aller Regel der Taktgeber des Geräts und nicht etwa die via NTP ermittelte Systemzeit.

Der Fingerprinter erfasst nun die Differenzen zwischen den Absende-Zeitstempeln eines Clients. Diese vergleicht er mit den Differenzen der Empfangszeitpunkte – und stellt Abweichungen fest. Diese Abweichungen manifestieren sich umso mehr, je länger der Fingerprinter den Messzeitraum wählt. Plottet man die Abweichungen in ein Zeitachsen-Diagramm, erhält man eine Linie mit individueller Steigung. Diese Steigung zeigt den Clock-Skew-Fingerprint über einen Zeitverlauf. Sie wird auch beim nächsten Besuch des Clients dieselbe individuelle Steigung aufweisen – und damit das Gerät wiedererkennbar machen.

„Unsere Messwerte liefern absolut zuverlässige Ergebnisse", versicherte ein Tracking-Experte, der anonym bleiben will. Sein Unternehmen plant, Clock-Skew-Fingerprinting insbesondere dann einzusetzen, um mobile Endgeräte zu tracken, bei denen der Einsatz von Cookies zu viele Unschärfen produziert. Eine Gegenwehr der Nutzer mit gängiger Anti-Tracking-Software wäre de facto sinnlos, weil die Tracking-Methode direkt auf die Hardware durchgreift. Um das Fingerprinting zu verhindern, müssten die TCP-Zeitstempel unterdrückt werden, was technisch eine simple Angelegenheit ist. Doch dazu müsste man überhaupt erst einmal wissen, dass man verfolgt wird.

Dass Clock-Skew-Fingerprintring einwandfrei funktioniert, haben zuletzt drei Forscher der Universität Los Angeles (UCLA) 2012 in Experimenten bestätigt. Sie konnten probeweise 152 PCs, 48 virtuelle Maschinen und 10 Smartphones zuverlässig voneinander unterscheiden und wiedererkennen. Allerdings benannten sie auch Unsicherheitsfaktoren: Eine Rolle hat dem veröffentlichten Bericht zufolge beispielsweise die Umgebungstemperatur gespielt.

Marketing-Druck kontra Datenschutz

Die Diskussion ums Nutzer-Tracking auf den Einsatz von Cookies zu reduzieren greift mittlerweile viel zu kurz. Im Kern geht es darum, ob der Nutzer dem Werber oder dem Website-Betreiber – unabhängig von der eingesetzten Technik – das Recht einräumen muss, ein Profil von ihm zu bilden oder eben nicht. Es ist absurd: Weitere Hindernisse beim Cookie-Einsatz spielen ausgerechnet Facebook, Google und anderen starken Anbietern in die Hände, weil die über ein Dauer-Login ihrer Nutzer ohnehin gut tracken können.

„Die großen Werbenetzwerke spielen möglichst viele Tracking-Verfahren parallel aus, weil sie an der exakten Messung der Conversion interessiert sind", erläutert Markus Kellermann, Experte für Affiliate-Marketing (Kaufvermittlung). Als Conversion bezeichnen Marketing-Fachleute die Wandlung eines Interessenten in einen Käufer. Coversion-Tracking ist ein wichtiger Mechanismus, weil die Affiliate-Netzwerke erheblichen Aufwand betreiben, um den Nutzer bei dessen Google-Recherchen abzuholen und zum passenden Angebot zu führen. Da die Affiliates in der Regel nur bei Kaufabschluss bezahlt werden, ist hier das Tracking wichtig.

Auch der permanente Preisverfall bei der klassischen Banner-Werbung zwingt die Online-Reklameindustrie, die ausgetretenen Tracking-Pfade zu verlassen. Jedermann ist inzwischen klar, dass er einer permanenten Rasterfahndung der Werber unterliegt. Methoden wie Canvas- und Clock-Skew-Fingerprinting, die kaum bekannt, nie in Nutzungsbedingungen erwähnt und schon gar nicht vom Nutzer abschaltbar sind, erhöhen das Misstrauen weiter. (hob)

Literatur

[1] The web never forgets: Persistent tracking mechanisms in the wild, https://secure-homes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

[2] Pixel Perfect: Fingerprinting Canvas in HTML5, http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf

Your knowledge.
Your people.
Your future.

HOB
Secure Business Connectivity

Security Powered by HOB

Umfassende Remote-Access Lösungen für alle Einsatzzwecke, alle Betriebssysteme, alle Geräte, auch Mobile Devices

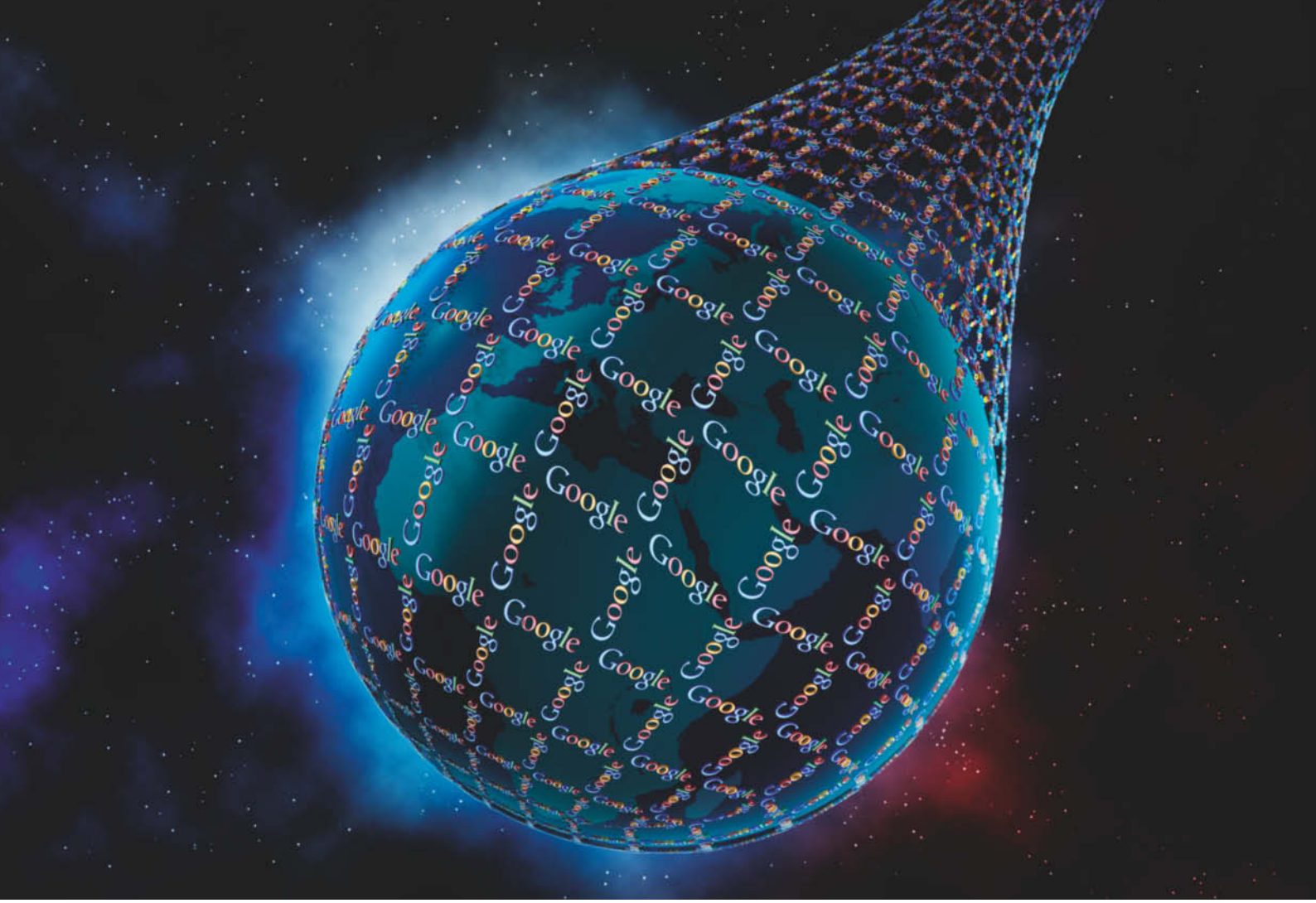
- Kostenersparnis durch clientless; keine Installation am Client
- Absolut sicher, nachgewiesen durch Zertifizierung durch das BSI nach **Common Criteria EAL 4+**

HOB RD VPN
Die umfassende SSL VPN Komplettlösung

HOBLink VPN
Modulare IPsec Connectivity

Vereinbaren Sie ein unverbindliches Beratungsgespräch!
Tel.: 09103-715-3715 E-Mail: marketing@hob.de

www.hob.de



Jo Bager

Netzmacht Google

Google steuert mit seiner Suchmaschine die weltweiten Surfer-Ströme, dominiert die Online-Werbung, kontrolliert mit seiner Plattform Android den Smartphone-Markt und setzt mit seiner immensen Entwickler-Power technische Standards im Web. Jetzt macht sich der Online-Riese daran, das Internet der Dinge zu erobern.

Viertel nach fünf am Nachmittag. Mein Handy vibriert. Google Now meldet: „Fahrtzeit nach Hause: 21 Minuten“. Die etwaige Aufbruchszeit, die Fahrtzeit, das Verkehrsmittel Fahrrad und das Ziel stimmen. Aber woher weiß Google das? Ich habe Google meine Adresse nie gegeben und auch so etwas wie meine Arbeitszeit nirgendwo hinterlegt.

Offenbar kennt Google mich verdammt gut. Ich benutze ein Android-Smartphone, die GPS-Lokalisierung habe ich oft eingeschaltet. Anscheinend hat Google oft genug mitgeschnitten, wann ich mich wo aufhalte und von wo nach wo ich fahre, und daraus auf meine Heim- und Arbeitsadresse geschlossen. „Das Ziel von Google ist es, die Informationen der Welt zu organisieren und für alle zu jeder Zeit zugänglich und nützlich zu machen.“ – Googles Mission klang lange Zeit wie ein hehres, abstraktes Ziel. Heute klingt das Motto fast wie eine Drohung.

Google ist zu einem Riesen gewachsen, ohne den mittlerweile kaum etwas geht im Web und im Mobilfunkmarkt – und der jeden Tag größer wird. Wir Google-Nutzer versorgen ihn ja gerne mit unseren Informationen. Die Suche, Android, YouTube und Co. sind einfach zu attraktiv, um ganz auf Google zu verzichten.

Machtfaktor Suche

Der zentrale Hebel für Googles Dominanz ist die Suchmaschine. In etlichen Ländern ist „Suchen im Internet“ gleichbedeutend mit googeln. In Europa etwa liegt der Marktanteil bei 92, weltweit bei mehr als 70 Prozent. Aus dieser Dominanz ergibt sich die schlichte Wahrheit: Wen Googles Suche nicht findet, der existiert nicht im Web. Wer also eine Website betreibt, muss Googles Regeln einhalten. Google gibt vor, wie eine gut gestaltete Seite auszusehen hat und was als Spam aussortiert wird. Webmaster, die sich nicht daran halten, müssen damit rechnen, von Google abgestraft und auf schlechte Ränge in den Suchergebnisseiten verbannt zu werden, die niemand anklickt.

Für seine Benutzer ist die Suchmaschine eine Art Vorkoster. Da sie in der Regel nur die Treffer der ersten zwei, drei Suchergebnisseiten abrufen, entscheidet Googles Ranking, welche Seiten sie zu einem

bestimmten Suchbegriff sehen und besuchen. Als meistfrequentierte Site schlechthin dirigiert Google so die weltweiten Surferströme im Netz. Mit anderen Worten: Der Suchmaschinenbetreiber kontrolliert den Zugang zum Weltwissen im Web: eine unvergleichliche Machtposition.

Und Google setzt alles daran, seine Besuchermassen auf den eigenen Seiten zu halten; der Suchende soll finden und bleiben. Die Suchergebnisseiten zeigen immer mehr Inhalte an, die die Fragen der Benutzer direkt beantworten. Dazu bettet Google auch Inhalte aus seinen anderen Diensten in die Suchergebnisse ein, seien es Karten, News aus dem eigenen Nachrichtenaggregator oder Produktlistings aus Google Shopping. Die einstige Navigationshilfe für das gesamte Web mutiert zum Portal, das die Besucher eng an sich bindet.

„Foul!", haben daher bereits 2010 mehrere Konkurrenten geschrien. Sie beschwerten sich bei der EU-Kommission über Google, die daraufhin ein Wettbewerbsverfahren eingeleitet hat. Derzeit ist der Status des Verfahrens unklar.

Es läuft wohl darauf hinaus, dass Google auf seinen Suchergebnisseiten Inhalten der Konkurrenz Platz einräumen muss – ein Novum. Der Suchmaschinenbetreiber wird die Ergebnisse fremder Spezialsuchdienste, etwa für Karten, Reisen oder Produkte, prominenter in den eigenen Ergebnissen platzieren und Angebote aus eigenen Spezialsuchmaschinen klarer von den „normalen" Suchergebnissen abgrenzen. Die Vormachtstellung der eigenen Inhalte wird so allerdings nur ein kleines Stück geschmälert, und das auch nur in der EU.

Geldmaschine Werbung

Google kann sich diese kleinen Zugeständnisse leisten, denn das Unternehmen schwimmt in Geld. Knapp 19 Milliarden Euro hatte der Konzern am Ende des Geschäftsjahrs 2013 auf der hohen Kante, plus 39,8 Milliarden US-Dollar in frei verkäuflichen Wertpapieren. Etwa 13 Milliarden Euro Gewinn hat Google allein im vergangenen Jahr erwirtschaftet. An der Börse ist Google nach Apple bereits das zweitwertvollste Unternehmen, und der Abstand schmilzt.

Werbung ist dabei Googles wichtigste Einnahmequelle. Etwa neunzig Prozent seiner Umsätze macht Google mit Reklame. Werbung auf eigenen Webseiten trägt dabei zu zwei Dritteln, die Vermarktung von Werbeflächen auf den Webseiten Dritter zu gut zwanzig Prozent zu den Umsätzen bei. Der Anteil der Einnahmen aus der Werbung auf Dritt-Sites sank zuletzt zwar. In einem anderen, sehr schnell wachsenden Markt könnte Google aber schon bald wieder Boden gutmachen: Googles Anteil am Mobil-Werbekuchen liegt bei mehr als 50 Prozent.

Rund um die Suchmaschine hat Google ein beachtliches Ökosystem mit Dutzenden Diensten geschaffen, angefangen bei Mail über Docs und Maps bis hin zu News und Translate. Für die wenigsten dieser Angebote nimmt das Unternehmen Geld. Google Enterprise etwa, ein Firmenpaket aus Gmail, Drive, Docs und Hangouts, kostet eine monatliche Gebühr. Der Großteil aller Dienste ist aber gratis. Viele Angebote finanzieren sich über eingeblendete Bannerwerbung.

Ein besonders heller Stern im Google-Kosmos ist der Videodienst YouTube. Die Plattform ist mittlerweile die am dritthäufigsten besuchte weltweit, nach der Mutter Google und Facebook. Mehr als eine Milliarde Besucher verzeichnet YouTube monatlich. Ein Teil des Erfolgs ist hausgemacht: 100 Millionen US-Dollar investierte Google in ein Förderprogramm für Videokanäle auf YouTube, weitere 200 Millionen ließ das Unternehmen an Werbekosten für solche Original-Channels springen. Offensichtlich war das Geld gut angelegt: 5,6 Milliarden US-Dollar setzte YouTube im letzten Geschäftsjahr mit Werbung um.

Bei einigen Diensten verzichtet der Werbekonzern sogar auf Werbung. Offenbar will Google dort den Benutzer nicht ablenken, etwa bei Docs oder den Angeboten für die Webmaster. Eine Gegenleistung erhält Google aber dennoch: Jeder zusätzliche Dienst, den ein Anwender einsetzt, bindet ihn stärker an das Unternehmen. Warum einen Mailer, ein soziales Netzwerk, einen Kalender oder ein Fotoalbum woanders nutzen, wenn man ohnehin schon einen Google-Account hat und die Dienste bei Google nichts kosten?

Mit der Nutzung jedes einzelnen Dienstes fallen zudem Daten an, die das riesige Werbeunternehmen zu nutzen weiß: Je mehr es über den einzelnen Anwender an Informationen aus den unterschiedlichen Diensten zusammentragen kann, desto zielgerichteter kann es ihm Werbung präsentieren.

Geballte Entwickler-Power

Google ist der weltweit attraktivste Arbeitgeber. Nach einer Erhebung der schwedischen Unternehmensberatung Universum aus dem Jahr 2013 unter internationalen Studierenden würden die meisten gerne bei Google anfangen. Das Unternehmen ist schon seit Jahren derart beliebt – und kann sich aus jedem Jahrgang die besten Absolventen herauspicken.

Wer erst einmal bei Google arbeitet, wird gehegt und gepflegt. Angefangen bei der nerdigen Büro-Ausstattung über kostenloses Essen und Gratismassagen – Google tut alles, damit sich seine klugen Köpfe wohlfühlen. Dazu gehört auch, dass Entwickler 20 Prozent ihrer Arbeitszeit in eigene Projekte stecken dürfen.

Angefangen bei der Hardware der Server, über die Software für den Betrieb der Dienste bis hin zu vielen Anwendungen für den Benutzer: Google entwickelt fast alles selbst –

Google Now

Googles Assistenzdienst Now zeigt schon heute, wie gut Google darin ist, Daten seiner Nutzer und aus der Cloud zusammenzutragen und auszuwerten. Abhängig von seinem aktuellen Standort und der zu erwarteten Fahrtzeit erinnert es den Nutzer zum Beispiel rechtzeitig an seine Treffen.

und wird dabei zum Motor der gesamten Branche. Das beste Beispiel dafür ist Chrome. Google war Mitte der Nuller Jahre mit der Performance der bestehenden Browser nicht zufrieden. Für seine Web-Dienste benötigte es Browser, die JavaScript schneller und besser ausführen können als die damals vorherrschenden Firefox und Internet Explorer.

Deshalb entwickelte Google eine eigene Alternative: Chrome. Es dauerte nicht lange, bis Chrome die Konkurrenz in puncto Performance und Funktionsumfang abhängte. Irgendwann gab Google mit Chrome den Takt bei der Browser-Entwicklung vor. Etwa alle zwei Wochen kommt bis heute ein neues Chrome-Release auf den Markt.

Das Tempo hat sich ausgezahlt: Chrome führt die weltweiten Browser-Statistiken mittlerweile mit einem Marktanteil von 48,7 Prozent an, vor Internet Explorer mit 23,0, Firefox mit 19,6 und Safari mit 4,9 Prozent.

Politik mit Technik

Seine große Programmier-Manpower kann Google einsetzen, um die Entwicklung strategischer Projekte in die gewünschte Richtung zu lenken. So nutzte Chrome lange Zeit die Rendering Engine WebKit, die auch in Apples Safari ihren Dienst verrichtet und an der Apple maßgeblich mitentwickelt. Im April 2013 verkündete Google dann, das Chrome zugrunde liegende Chromium-Projekt auf eine eigene Rendering Engine namens Blink umzustellen.

Mittlerweile verrichtet Blink nicht nur in Chrome seinen Dienst, sondern auch in Opera und anderen auf Chromium aufsetzenden Browsern; in die Qt-Bibliothek für grafische Bedienoberflächen soll Blink integriert werden. Blink ist also dabei, WebKit als maßgebliche Rendering Engine im Netz abzulösen: Statt diese Kernkomponente für Browser mit Apple-Entwicklern gemeinsam voranzutreiben, hat Google jetzt bei Blink die Federführung. Google gibt sich gerne offen; Blink ist wie der Chrome-Kern Chromium nach wie vor ein Open-Source-Projekt. Doch kann man sich schlecht vorstellen, dass irgendeine Funktion in die beiden Projekte Einzug hält, die nicht von Google abgenickt wurde.

Bei anderen Produkten hat Google auch schon mal die Unterstützung offener Standards eingestellt, wenn das den eigenen Zwecken diente. So beendete Google Mitte 2013 die XMPP-Unterstützung seines Chat-Clients Hangouts. Das Jabber-Protokoll XMPP hat unter allen Chat-Protokollen die breiteste Unterstützung. Sogar Facebook nutzt es, und auch Googles eigener Messenger Talk hatte per XMPP kommuniziert. Er wurde dann aber durch das proprietäre Hangouts abgelöst.

Hiergeblieben

Google beantwortet immer mehr Suchanfragen direkt, etwa durch einen Kasten rechts neben den Suchergebnissen. Wer zum Beispiel nach „Angela Merkel“ sucht, sieht in der rechten Spalte einen Kasten mit Basisinformationen. Zwei Sätze umreißen das Thema. Darunter stehen in Stichpunktform einige Kerndaten: Geburtsdatum und -Ort, Beruf, Partei, der Name ihres Manns, ihrer Eltern und ihrer Geschwister.

Der sogenannte Knowledge Graph ist dafür verantwortlich. Er erscheint unter anderem bei der Suche nach Ländern, Städten, Prominenten, Filmen und Serien und soll die Suche auf Basis semantischer Informationen verbessern. Der Knowledge Graph umfasst eine Datenbank des Weltwissens, die Hunderttausende Objekte und Personen der Welt und ihre Beziehungen zueinander umfasst. Google benennt die Quellen. Größtenteils stammen die textlichen Kurzinformationen aus der Wikipedia; Google baut die Anzahl der Quellen aber aus.

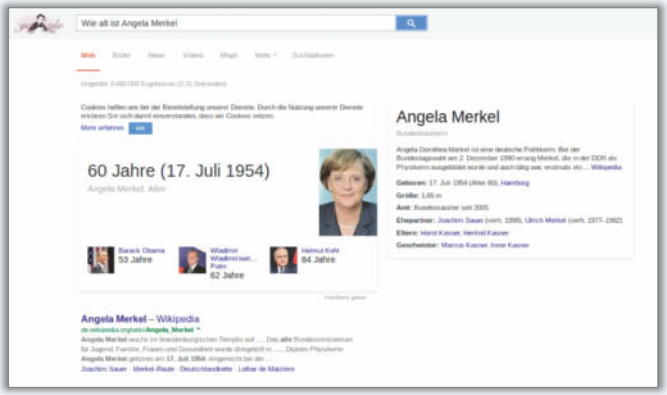
Wer es genauer wissen will und nicht nur den Namen der Kanzlerin sucht, sondern „Geburtsdatum Angela Merkel“ eingibt, sieht außer dem Knowledge-Graph-Kasten oberhalb der Trefferliste sofort die Antwort: Es ist der 17. Juli 1954. Diese Direktantworten, auch Answer Boxes genannt, erscheinen bei einer Reihe von Abfragetypen. Dazu gehören die Geburtsdaten von Prominenten, architektonische („Höhe Eiffelturm“) oder kulturelle Fakten („Regisseur Pulp Fiction“), die Einwohnerzahl von Städten, das Alter von Prominenten, der Aktienkurs von DAX-Konzernen („Kurs Siemens“), das Wetter und aktuelle Fußball-Ergebnisse („Bundesliga Ergebnisse“). Außerdem erscheinen sie, wenn man vor einen Begriff das Wort „Definition“ eingibt.

Für Jens Heickmann von SEOlytics sollen die Direktantworten höhere Werbeerlöse bringen: „Je länger ein User im Google-Imperium bleibt und sich darin bewegt, desto häufiger kann ihm Werbung präsentiert werden.“ Klickt man auf Links innerhalb des Knowledge Graphs, zum Beispiel auf den Geburtsort und die Filme von Quentin Tarantino, werden wiederum neue Google-Suchen ausgelöst – und es gibt eine neue Wahrscheinlichkeit, dass ein Nutzer auf eine Google-Anzeige klickt.

Zudem glaubt Heickmann, dass Google so die Wahrnehmung der Nutzer steuern will. „Mit dem Knowledge Graph hat Google die zweispaltigen Suchergebnisseiten eingeführt und den User daran gewöhnt, dass auf der rechten Seite interessante Informationen dargestellt werden.“ Lösen Suchbegriffe Google Ads aus, erscheinen die Anzeigen genau dort, wo in anderen Fällen der Knowledge Graph oder die Sofortantwort-Box erscheint.

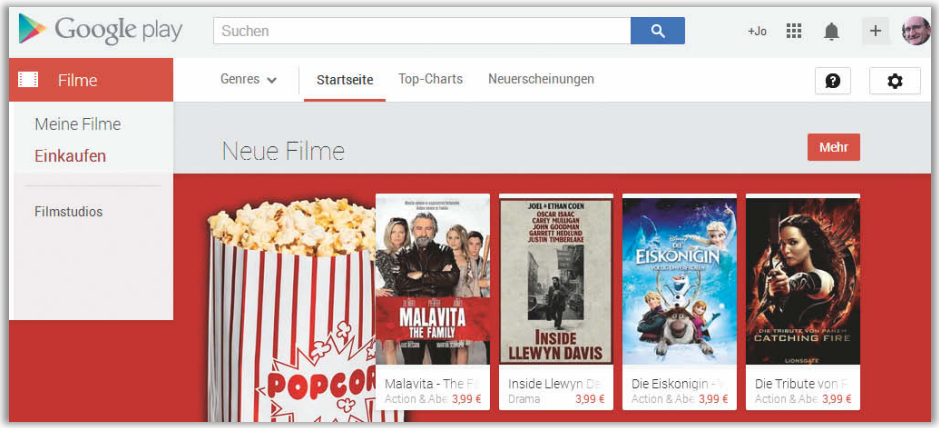
Für den Rest der Web-Welt dürfte es auf jeden Fall eine schlechte Nachricht sein, dass Google immer mehr Fragen selbst beantwortet. Anderen Website-Betreibern gehen auf diese Weise Besucher verloren. Es gibt zum Beispiel Hinweise darauf, dass der Knowledge Graph zu einem Traffic-Verlust bei Wikipedia geführt hat. Im Jahr 2013 hat Wikipedia im Vergleich zum Vorjahr 10 Prozent seines Traffics verloren, in Deutschland sogar 17 Prozent.

(Stefan Mey)



Weggehen nicht notwendig: Google versucht, Fragen zunehmend selbst zu beantworten.

Obwohl Android erst nach iOS gestartet ist, liegt es heute weit vor Apples Konkurrenzsystem und beschert Google, etwa via Play Store, satte Gewinne.



Unbeliebt hat sich Google mit dem Einstellen des Reader und der personalisierbaren Startseite igoogle gemacht. Statt wie bisher auf offene Standards wie RSS für den Austausch von Nachrichten-Streams zu setzen, wollte das Unternehmen so offenbar seine Nutzer dazu bewegen, das soziale Netzwerk Google+ als Nachrichtenzentrale zu nutzen. Einen RSS-Feed, mit dem Benutzer ihre Google+-Updates mit einem anderen Programm als dem Google+-Webfrontend abrufen können, stellt Google nach wie vor nicht bereit.

Am aggressivsten hat Google Standards bisher gegen den Konkurrenten Microsoft und dessen Plattform Windows Phone eingesetzt. Indem es Mitte 2013 die Unterstützung des Protokolls ActiveSync für den Austausch von Kalenderdaten und Kontakten abbrach, waren die Nutzer von Smartphones mit Microsofts Betriebssystem von der Nutzung von Googles Diensten abgeschnitten.

Lobbyismus auf allen Kanälen

Als großer Betreiber von Web-Diensten, aber auch als Browser-Hersteller, hat sich Google die Möglichkeit erarbeitet, in allen großen Gremien, in denen es um Netz- und Webstandards geht, ein gehöriges Wörtchen mitzureden. Nicht selten vertritt der Suchmaschinenhersteller seine Interessen sogar mit mehr Mitarbeitern als jedes andere Unternehmen, wenn es ihm um etwas geht.

Google ist neben Mozilla und Opera federführend bei der Entwicklung von WebRTC, einem Technikbündel für Echtzeitkommunikation im Browser. Das Unternehmen steuert hierzu den Video-Codec VP8 bei, den es erworben und unter eine offene Lizenz gestellt hat. Und Teile des Web-Protokolls HTTP will Google mit einem eigenen Protokoll ablösen, SPDY. Google hat SPDY bei der IETF als Vorschlag für die Standardisierung eingereicht. Gleichzeitig schafft es aber bereits Fakten: Die eigenen Dienste unterstützen SPDY bereits ebenso wie Chrome. Mittlerweile beherrschen Firefox, Opera und Internet Explorer ebenfalls das neue Protokoll.

Auch auf klassischen, politischen Kanälen betreibt Google viel Lobby-Arbeit. So gab das Unternehmen nach einer Analyse der Verbraucherschutzseite consumer watchdog im Jahr 2013 14,06 Millionen Dollar dafür aus. Damit lagen die Lobby-Ausgaben um 3,57 Millionen Dollar höher als beim Rivalen Microsoft und höher als die von Apple, Amazon und Facebook zusammen.

Für seine Lobby-Tätigkeit bei der EU gab Google im Jahr 2012 immerhin gut eine Million Euro aus, so die neueste Zahl des EU-Transparenz-Registers. Auch in Deutschland hat Google bereits Millionen für Lobby-Zwecke ausgegeben. So finanziert Google seit 2010 die Denkfabrik Collaboratory, die „die Wechselwirkungen zwischen Internet und Gesellschaft“ untersuchen soll. Außerdem unterstützt das Unternehmen mit 4,5 Millionen Euro über drei Jahre hinweg den Aufbau einer wissenschaftlichen Einrichtung zum Thema „Internet und Gesellschaft“ an der Humboldt-Universität in Berlin. Seit 2008 unterhält Google in Berlin zudem ein eigenes Büro, zu dessen Aufgaben unter anderem „Legal & Government Relations“ zählt.

Europa als Ganzes und insbesondere Deutschland ist allerdings Google-kritischer eingestellt als das Heimatland. Trotz aller Lobby-Aktivitäten konnte Google weder die bereits erwähnten EU-Wettbewerbssanktionen verhindern noch das deutsche Leistungsschutzrecht – ein Gesetz, das im Grunde ausschließlich gegen Google News gemünzt ist. Es ist auf Betreiben von Presseverlagen entstanden, die sich die Verwendung auch von kleinen Textabschnitten in Google News vergüten lassen wollten. In seiner aktuellen Version ist das Leistungsschutzrecht allerdings so schwammig formuliert, dass Google bis dato keinen Cent an die Verlage gezahlt hat.

Unter „Lobby-Arbeit für das freie Netz“ kann Google auch seine Zahlungen an die Mozilla Foundation verbuchen. Denn Google ist der mit Abstand größte Geldgeber der Stiftung. Alleine im Jahr 2012 hat Google etwa 280 Millionen Dollar an Mozilla gezahlt für die Integration der Suche in Firefox. Eine prekäre Situation für Mozilla: Als Konkurrent auf dem Browsermarkt und mit Firefox OS auch bei den Mobilbetriebssystemen hängt man an der Finanzspritze aus Mountain View. Diese Abhängigkeit unterminiert zudem Mozillas Status als unabhängiger Anwalt für freie Webstandards.

Der neue Gorilla

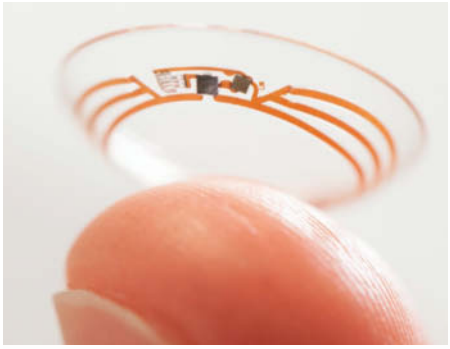
Ein alter Witz über Microsoft geht so: „Wo setzt sich ein 800 Kilo schwerer Gorilla hin? Wo er will.“ Microsoft war einmal dieser Gorilla der IT-Branche. Das Unternehmen setzte mit seinen Betriebssystemen die technischen Standards der Branche. Es konnte in aller Ruhe abwarten, wo sich ein interessanter Markt entwickelt und ihn dann von hinten aufrollen, wie es das etwa bei Word und Excel geschafft hat.

Diese Position hat Microsoft längst an Google verloren. Nicht nur bei der Suchmaschine, sondern auch beim Browser, mit seinem Mobilbetriebssystem Windows Phone und bei vielen Web-Diensten hinkt Microsoft Google hinterher – dem neuen Gorilla. Sollte doch einmal ein Konkurrent oder ein Produkt eine Bedrohung für Google darstellen, ist der Suchmaschinenkonzern so beweglich, dass er das kontern kann.

So musste Google zum Beispiel etwas unternehmen, als Apple 2007 das iPhone vorstellte. Dieses in vielem neuartige Gerät, so viel war sofort klar, würde den Mobilfunkmarkt verändern. Apple stellte die Hardware her und kontrollierte auch den App Store, konnte also bestimmen, wer seine Apps auf dem iPhone veröffentlichen darf. Apple nutzte das auch zugunsten eigener Apps aus und ließ zum Beispiel fremde Browser wie Googles Chrome zunächst nicht zu.

Riesenerfolg Android

Google musste also dagegenhalten. Es gründete mit Dutzenden von Partnern die Open Handset Alliance, mit der es ein Smartphone-Betriebssystem namens Android entwickelte. Den Grundstock dafür, das von Andy Rubin gegründete Unternehmen Android, hatte Google sich praktischerweise bereits im Jahr 2005 einverleibt. Vorangetrieben und kontrolliert durch Google wurde Android zu einer einzigen Erfolgsgeschichte: Derzeit werden etwa 80 Prozent aller neuen Smartphones mit Android ausgeliefert, und auch



Näher am Menschen geht es nicht: Googles Diabetiker-Kontaktlinse misst den Blutzuckerspiegel direkt auf dem Auge.

bei den Tablet-Verkäufen lag Android im Jahr 2013 erstmals vor iOS.

Im Prinzip ist Android ein offenes System; jeder kann auf Basis des Quellcodes eigene Android-Versionen herausbringen. In der Praxis findet das aber nur sehr eingeschränkt statt. Google gibt stattdessen die Richtung der Android-Entwicklung vor. Apps, die Google nicht passen, etwa Werbeblocker, fliegen aus dem Play Store. Google betätigt sich wie eine Android-Ordnungskraft und versucht, die Gerätehersteller dazu zu bewegen, ihre Geräte möglichst schnell mit Updates zu versorgen – und somit auch mit den neuesten Versionen von Googles Apps.

Grundsätzlich gilt, dass Android auch ohne Googles Anwendungen ausgeliefert werden kann. Amazon zum Beispiel ersetzt bei seinen Kindles den Play Store durch einen eigenen App-Laden. In der Praxis aber wird fast jedes Android-Gerät mit etwa einem Dutzend Google-Apps ausgeliefert. Im Laufe der Android-Entwicklung sind immer mehr dazugekommen; Google macht sich auch hier breit. Android ist mittlerweile ein integraler Bestandteil von Googles Ökosystem geworden, mit Google Now als sichtbarstem Element auf dem Homescreen.

Und Android erweist sich zudem als immer lukrativere Einnahmequelle. So hat Google gemäß aktueller Schätzungen mit Apps, Musik, Videos und anderen Inhalten aus dem Play Store bereits weit mehr als eine Milliarde Euro Gewinn gemacht. Das entspräche einem Großteil der „sonstigen" Gewinne neben der Werbung. Schon heute werden mehr Apps und Updates in den Play Store hochgeladen als in den App Store.

Facebook gekontert

Ein zweiter wichtiger Wettbewerber, auf den Google reagieren musste, war Facebook. Irgendwann im Jahr 2010 muss Facebook zu groß geworden, zu schnell gewachsen sein. Mark Zuckerbergs soziales Netzwerk war dabei, das Suchmaschinen-Unternehmen als wichtigsten Wegweiser im Netz zu bedrohen – und als Werbeplattform. Google musste sich etwas einfallen lassen und brachte mit einem Riesenaufwand Google+ an den Start.

Anfangs erweiterte Google sein soziales Netzwerk täglich um neue Funktionen. Später wurde Google+ eng mit anderen Diensten verknüpft, etwa mit der Suche. Irgendwann benötigte man einen Google+-Account, wenn man im Play Store oder bei YouTube kommentieren wollte. So wurden Googles sozialem Netz nach und nach immer neue Benutzer zugeführt.

Googles Plattform ist immer noch nicht so erfolgreich wie Facebook. Letzte Zahlen sprechen von gut 500 Millionen Nutzern, im Vergleich zu knapp 1,3 Milliarden Facebook-Mitgliedern. Google hat Facebook also nicht so spektakulär abgefangen oder gar überholt, wie Android es mit iOS schaffte. Aber Google+ ist alles andere als die von Kritikern immer wieder an die Wand gemalte Geisterstadt. Das belegen die Aufrufzahlen, die Google seit Kurzem für jedes Profil veröffentlicht. Und in wirtschaftlicher Hinsicht scheint Facebook, das im vergangenen Geschäftsjahr vergleichsweise bescheidene 2,8 Milliarden Dollar erwirtschaftete, für Google nach wie vor keine Gefahr zu sein.

Frühjahrsputzaktionen ...

Mit seinen etwa 50 000 Mitarbeitern ist Google alles andere als ein Start-up. In den letzten Jahren haben sich immer mal wieder vereinzelt ehemalige Mitarbeiter zu Wort gemeldet, die Google enttäuscht den Rücken gekehrt haben, weil sie das Gefühl hatten, dort nicht genug bewegen zu können. Zu Frust unter Mitarbeitern könnten auch die Frühjahrsputzaktionen geführt haben, bei denen Google schon seit mehreren Jahren Dienste schließt.

Kurz nachdem Larry Page im Jahr 2011 das Ruder bei Google wieder von Eric Schmidt übernommen hatte, begann das Unternehmen, nach und nach etliche Dienste einzustellen, die nicht hinreichend erfolgreich erschienen oder nicht mehr zum restlichen Portfolio passten. Dazu zählen neben vielen kleinen, unbekannten Angeboten auch große Projekte wie der Messenger- und Teamwork-Service Wave sowie die Wissensplattform Knol, die mal eine Art Wikipedia-Alternative werden sollte.

Das Ausprobieren – und Verwerfen bei Misserfolg – scheint fest in der Google-DNA verankert zu sein. Scheitern ist keine Schande, sondern gehört dazu. Wenn sich also herausstellt, dass ein Smartphone-Unternehmen wie Motorola, das Google erst im Mai 2012 gekauft hat, nicht zum Rest des Konzerns passt – dann wird es eben Anfang 2014 wieder verkauft. In diesem Punkt scheint sich Google die Kreativität und Flexibilität eines Start-ups erhalten zu haben.

... und Experimente allerorten

Google hat nach Informationen des Spiegel alleine 2013 acht Milliarden Euro in Forschung investiert. Das Unternehmen forscht in vielen Gebieten, in denen man den Suchmaschinen-, Werbe- und Webdienste-Giganten nicht erwarten würde. Bei allen Forschungsvorhaben ist Google sehr verschlossen und verrät nicht, welche konkreten Produkte das Unternehmen anvisiert. Mitunter entstehen deshalb wilde Spekulationen darüber, wo es hinwill.

Auf jeden Fall will Google noch mehr über jeden und alles wissen. Was es bereits über jeden Einzelnen weiß, lässt sich heute zum Beispiel an Google Now festmachen, das die Adressen von Arbeitsplatz und Wohnung des Benutzers selbstständig erkennt und ihn rechtzeitig vor einem Termin mit der zu erwartenden Fahrtzeit zu der jeweiligen Adresse benachrichtigt.

Wie gut das Unternehmen bereits Teile des Weltwissens verarbeiten kann, zeigt die Suche, die automatisch Synonyme erkennt, Fehler verbessert und bestimmte Fragen direkt beantwortet. Google will aber noch mehr. So forscht das Unternehmen im Projekt Google Brain daran, menschliches Lernen und Intelligenz zu imitieren.

Ein weiteres Ziel ist es, den Menschen im wörtlichen Sinn mehr auf die Pelle zu rücken: Wenn der Konsument schon nicht bereit ist, permanent eine Google-Brille auf der Nase zu tragen, dann kauft er vielleicht eine Uhr oder einen Aktivitätstracker mit einer speziell darauf zugeschnittenen Android-Version namens Android Wear. Im Extremfall erfasst Google wichtige Körperparameter sogar direkt, wie bei der am Jahresanfang vorgestellten Kontaktlinse, die bei Diabetes-Patienten den Blutzuckerspiegel misst: Google wird so zum unverzichtbaren Begleiter auf Schritt und Tritt.

Näher zu den Menschen scheint Google auch mit der Übernahme des Herstellers Nest rücken zu wollen, der intelligente Thermostate und Rauchmelder herstellt. Das Unternehmen hat zwar mit den Android-Geräten und YouTube-Apps auf Smart TVs bereits den Weg ins Wohnzimmer gefunden. Über die intelligenten Thermostate kann es aber Informationslücken schließen, die entstehen, wenn der Nutzer mal von seiner Unterhaltungselektronik ablässt, zum Beispiel: Von wann bis wann ist er genau zu Hause?

Google ist mit Android oder in Form von Maps in den Entertainmentsystemen schon