INTER AKTIV

MultiMedia News

Sonderausgabe 2014

www.interaktiv-muc.de
www.facebook.com/interaktiv.muc

Who's watching you?

Sicher ist sicher

„Ich habe doch nichts zu verbergen", das ist einer der am häufigsten gehörten Sätze, wenn es um Datenschutz und Überwachung geht. Doch ist das wirklich ein gutes Argument? Müsste man nicht vielmehr den Spieß umdrehen und fragen: „Was geht die das an?" Und konkret nachfragen: „Wer sind DIE eigentlich?"

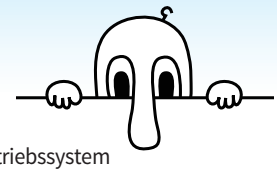
Wer ist denn interessiert an unseren privaten Daten?

Digitale Großkonzerne:
Wir haben es im Netz und auf Smartphones mit einigen wenigen Konzernen zu tun, die in den vergangenen Jahren unheimlich groß geworden sind. Die drei bekanntesten Beispiele:

Apple startete 1976 als Hersteller von Heimcomputern. Der durchschlagende Erfolg stellte sich nach der Einführung der ersten iPods 2001 ein. In der Diskussion um den Schutz von persönlichen Daten befindet sich Apple spätestens, seitdem das Unternehmen den Dienst iCloud für seine Geräte anbietet, mit dem sich Daten über die Apple-Server synchronisieren lassen.

Facebook, im Jahr 2004 als soziales Netzwerk gestartet, hat später weitere populäre Dienste wie Instagram und WhatsApp aufgekauft. Bei seinem Börsengang im Mai 2012 erreichte Facebook einen Börsenwert von 107 Milliarden US-Dollar.

Google startete 1998 als Suchmaschine, entwickelte sich dann zu einem umfassenden Online-portal, zu dem u.a. die Videoplattform YouTube und das Betriebssystem Android gehören. Google und Apple gehören zu den wertvollsten börsennotierten Unternehmen der Welt.



Staatliche Geheimdienste:
Wie Edward Snowden im Juni 2013 enthüllte, geht die Neugierde der weltweiten Geheimdienste weit über das hinaus, was sich die meisten von uns vorstellen konnten. An sich ist es logisch, dass alle digital übertragenen Daten auch mitgelesen und überwacht werden können. Dennoch hatten nur die wenigsten Menschen erwartet, dass amerikanische und britische Geheimdienste tatsächlich auf sämtliche privaten Daten, Mails, Telefonate usw. zugreifen und diese elektronisch auswerten.

Was bringt es eigentlich, unendlich viele Daten zu speichern?

Nun, den Konzernen bringt es natürlich Geld, wie wir an den Börsenwerten sehen können. Immerhin haben wir hier aber tatsächlich die Möglichkeit, selbst zu entscheiden, welche Daten wir dort veröffentlichen möchten.
Bei den Geheimdiensten ist die Sache ganz anders gelagert, hier wird tatsächlich alles gescannt, was wir digital austauschen, ohne dass wir darauf Einfluss hätten, was wir preisgeben wollen. Jedoch verdienen die Geheimdienste kein Geld mit unseren Daten, sondern durchforsten sie wohl tatsächlich nur, um Verbrechen oder Terroranschläge zu verhindern. Ob es allerdings ein legitimer Weg ist, die komplette Bevölkerung unter Generalverdacht zu stellen und komplett zu überwachen, oder ob dadurch nicht staatliche Befugnisse missbraucht werden, das sei dahingestellt. Bedenklich ist jedoch, dass nun offensichtlich auch die deutschen Geheimdienste die Methoden der britischen und amerikanischen Dienste übernehmen: Auch der BND plant, soziale Netzwerke live zu überwachen.

Was tun?

Leider können wir uns gegen diese Totalüberwachung nur schlecht wehren: Wer digitale Medien und Online-Dienste nutzen möchte (denn die Vorteile dieser Dienste sind unbestritten), der muss sich wohl damit abfinden, dass die Anbieter und auch die Geheimdienste mitlesen. Dennoch gibt es einige Schutzmaßnahmen, z.B. durch Verschlüsselung der Kommunikation oder die Nutzung von Alternativen zu WhatsApp, Facebook und Google. Wir haben daher einige Tipps und Empfehlungen für dich zusammengestellt.

Viel Erfolg beim sicheren Surfen
wünscht die AG Interaktiv

Durchbrecht die Monopole

Alternativen zu den Giganten
Es muss nicht immer WhatsApp sein. Vielleicht auch mal Textsecure, Telegram oder Threema ausprobieren? Browser gibt es viele, teste doch mal Iron oder Opera. Es hat sich ausgegoogelt, auch über DuckDuckGo oder Ecosia kannst du das Netz durchsuchen.
Kaum zu glauben, aber wahr: Nicht nur auf YouTube gibt es Videos. Schaut doch mal auf Vimeo oder Veoh vorbei. Facebook gefällt Dir nicht mehr? Auch auf Diaspora kannst du Freunde finden.

Sperrzone für Unbefugte — So sicherst du dein Smartphone

SIM- und Displaysperre Es ist wichtig, dass du deine SIM-Karte durch eine PIN schützt und bei Verlust oder Diebstahl solltest du diese sofort sperren lassen. Die kostenlose Nummer dazu lautet 116 116. Außerdem ist eine Sperre für dein Display Pflicht, damit dein Smartphone, auch wenn es eingeschaltet ist, vor unbefugtem Zugriff geschützt ist. Diese beiden Sperren kannst du in deinem Smartphone unter „Einstellungen" > „Sicherheit" aktivieren.

Verschlüsselung Auf Smartphones gibt es eine Basisverschlüsselung, um bei Verlust deine persönlichen Daten zu schützen. Diese muss jedoch zum Beispiel bei Android-Geräten erst aktiviert werden.
Zur Verschlüsselungsfunktion kommst du so: Einstellungen > Sicherheit > Verschlüsselung > Telefon verschlüsseln. Aber Vorsicht: einmal verschlüsselt, immer verschlüsselt. D.h. wenn du die Verschlüsselung aufheben möchtest oder dein Passwort vergessen hast, hilft nur das Smartphone auf Werkseinstellung zurückzusetzen und alle deine Daten sind weg. So bekommt sie zwar kein Unbefugter in die Finger, aber auch du hast deine Daten verloren, falls du in der Vergangenheit kein Backup erstellt hast.

Surfen in öffentlichen Netzen Öffentliche WLAN-Hotspots ohne Passwort sind in der Regel nicht verschlüsselt. Das heißt, dass die meisten Daten, die du in einem offenen WLAN überträgst, ohne große Probleme von anderen Nutzerinnen und Nutzern im Netzwerk mitgelesen werden können.

Angreifer abwehren Nicht nur Computer können sich Viren einfangen oder gehackt werden, sondern auch Smartphones. Deshalb solltest du Apps nur aus vertrauenswürdigen Quellen herunterladen (z.B. Google Play oder App Store) und auch ein Antivirenprogramm solltest du auf deinem Smartphone installieren. Lese und prüfe vor der Installation auch die Datenschutzerklärung. Du wirst staunen, auf was so eine kleine App alles Zugriff hat.

TIPP Damit Apps z.B. nicht deinen Standort ermitteln können, solltest du unter Einstellungen > Nutzer > Standortzugriff den Standortzugriff deaktivieren. Wenn du dich dann doch einmal an einen bestimmten Ort navigieren lassen willst, kannst du den Standortzugriff immer noch vorübergehend aktivieren.

MultiMediaNews
Sonderausgabe 2014

Geheimnisse soll man schützen

Wir alle haben Geheimnisse und das ist auch gut so. Früher war es vielleicht das Tagebuch, heute sind es Dokumente auf deiner Festplatte. Das Tagebuch hat man verschlossen, den Computer kann man verschlüsseln. Es gibt Programme, die verändern die Daten so, dass der ursprüngliche Inhalt nicht mehr zu erkennen ist. Das funktioniert mit aufwendigen Rechenverfahren über einen individuellen elektronischen Schlüssel, geht aber ganz einfach. Und nur mit dem dazugehörigen Passwort lassen sich die Daten wieder entschlüsseln.
Es gibt mehrere Wege, Daten zu verschlüsseln. Informiere dich unter Wikipedia, Suchwort: Festplattenverschlüsselung.

Linktipps

www.lda.bayern.de | www.watchyourweb.de
www.datenparty.de | www.handysektor.de
www.checked4you.de | www.klicksafe.de
http://irights.info

Tipps für sichere Passwörter

Verwende für deine Passwörter keine Geburtsdaten, Postleitzahlen, Telefonnummern oder Namen von Haustieren oder von bekannten Personen.
Sichere Passwörter kombinieren Klein- und Großbuchstaben, Zahlen und Sonderzeichen.

TIPP

Auf passwordchart.com kannst du dir aus einem Wort ein sicheres Passwort inklusive Merkhilfe generieren lassen, die du ausdrucken kannst. Mit diesem Trick musst du dir nur einfache Passwörter merken, kannst aber für Anmeldungen auf Webseiten sehr komplizierte und kaum zu erratende Passwörter verwenden.

Passwort-Manager

Bequem ist es, Passwörter für Webseiten vom Passwort-Manager des Browsers speichern zu lassen. Dumm nur, wenn der Rechner dann geklaut wird oder sich jemand daran zu schaffen macht, wenn du gerade nicht hinschaust.
Bei bestimmten Browsern wie Firefox besteht die Möglichkeit, ein Masterpasswort zu vergeben, das du erst eingeben musst, um dem Browser das Laden eines gespeicherten Passworts zu erlauben. Somit kann sich niemand „mal schnell“ in deinem Namen auf einer Webseite einloggen, selbst wenn er Zugriff auf deinen Rechner hat.

TIPP

Wenn du es noch sicherer haben willst, verwende einen Password-Safe wie z.B. KeePass (http://keepass.info). In diesem kannst du deine Passwörter komplett verschlüsselt ablegen und bei Bedarf automatisch in die entsprechende Webseite einfügen lassen.

Geheim war gestern?

Nein, denn deine Adresse, Telefonnummer, Bankdaten oder Passwörter gehen erst einmal niemanden was an und gehören deshalb nicht in ein öffentliches, soziales Netzwerk, selbst wenn du dazu aufgefordert wirst!
Gehe immer sorgsam mit deinen persönlichen Daten um. Du gibst ja auch nicht jedem, den du triffst, deinen Schlüssel zu deiner Wohnung, oder? Überlege dir auch, ob du deinen richtigen Namen angeben musst. Wenn du wiedererkannt werden möchtest, dann kürze zumindest deinen Nachnamen ab (z.B. Laura M.).

Wer sieht was?

Nahezu alles kann man mit seinen „Freunden“ auf sozialen Netzwerken wie z.B. Facebook teilen. Dabei liegt es in deiner Verantwortung, die Privatsphäre-Einstellungen zu überprüfen. Du solltest darauf achten, welche Daten du mit welchen Personen teilst. Achte deshalb genau darauf, wer im Internet mit dir befreundet ist und sei vorsichtig bei Anfragen von Personen, die du nicht kennst.

Sie wissen, wer du bist, wo du bist und was du tust

Wie sicher sind eigentlich meine Daten?

Je mehr Dinge im Internet erledigt werden, desto einfacher ist es, deine Daten zu missbrauchen. Einen hundertprozentigen Datenschutz gibt es nicht! Jeder Besuch im Internet hinterlässt Spuren. Neueste Techniken erlauben es, Profile, besuchte Webseiten, den Verlauf deiner Einkäufe oder Beziehungen zu anderen Surfern, nachzuvollziehen. Leider werden diese Daten immer wieder illegal genutzt. Im Folgenden findest du einige Regeln und Tipps, wie du mit deinen persönlichen Daten im Internet umgehen solltest und wie du sie schützen kannst.

Anonym im Netz?

Leider nein. Sobald du auf eine Seite surfst, will diese wissen, wohin die Datenpakte gesendet werden sollen. Deshalb verfügt dein Computer – ähnlich zu deiner Postanschrift – über eine IP (Internetprotokoll)-Adresse. Somit weiß der Seitenanbieter wohin die Daten geschickt werden sollen. Wie lautet deine öffentliche IP-Nummer? Finde es heraus unter http://www.wieistmeineip.de/

Heartbleed

Es ist das visualisierte Zeichen für das Hacken von Millionen Online-Konten (E-Mail-Postfächer, Soziale Netzwerke etc.). Entdeckt wurde die Sicherheitslücke Anfang 2014. Bist vielleicht auch du betroffen? Deine E-Mail-Adresse beispielsweise kannst du überprüfen lassen unter https://www.sicherheitstest.bsi.de/#email.

Wähle deine Bilder sorgsam aus!

Sicher, in einem sozialen Netzwerk werden meistens auch Bilder hochgeladen. Aber Achtung! Erotische Fotos oder Fotos von Alkoholexzessen sind absolut tabu. Du würdest diese Bilder auch nicht in der Fußgängerzone aufhängen. Achte auch darauf, wer mit dir auf den Bildern abgebildet ist. Sind alle abgebildeten Personen mit der Veröffentlichung einverstanden? Hast du ihre Einwilligung eingeholt? Woher hast du die Bilder, die du ins Netz stellst? Bist du dir sicher, dass du sie auch veröffentlichen darfst? Wenn nicht, dann lass es. Denn ansonsten riskierst du eine Abmahnung, Klage oder sogar eine strafrechtliche Verfolgung

Räum hinter dir auf!

Wenn du ein Netzwerk nicht mehr nutzen möchtest, solltest du deine Mitgliedschaft beenden und dein Profil löschen.

Wehr dich!

Wenn du im Netz beleidigt oder gemobbt wirst, dann gilt: nicht darauf reagieren oder antworten! Denn das ist es, was der Angreifer erreichen will. Melde den Eintrag dem Betreiber der Website und hol dir Hilfe bei deinen Eltern, Lehrerinnen oder Lehrern. Auch die Weitergabe deiner Daten entgegen der Nutzungsbedingungen verstößt gegen deine Persönlichkeitsrechte. Gegen die Weitergabe deiner Daten kannst du widersprechen und deren Löschung verlangen.
Weitere wichtige Regeln kannst du unter den Linktipps nachlesen.

Impressum

MultiMediaNews erscheint im Auftrag der AG Interaktiv, www.interaktiv-muc.de

Redaktion: SIN – Studio im Netz
Gestaltung: Steffi Jentsch Kommunikations Design, Corporate Identity: Konrad Bayer, khargosh
Fotos: Titelseite: privat, Seite 2: Heartbleed CC Zero

Organisationsadresse: SIN – Studio im Netz e.V., Heiglhofstraße 1, 81377 München, www.sin-net.de

AG Interaktiv: Kinder- und Jugendmuseum München | Kreisjugendring München-Stadt | Kulturreferat | Medienzentrum München des JFF – Institut für Medienpädagogik in Forschung und Praxis | Münchner Volkshochschule | Pädagogische Aktion/SPIELkultur | Referat für Bildung und Sport/Pädagogisches Institut | SIN – Studio im Netz e.V. | Sozialreferat/Stadtjugendamt München | Spiellandschaft Stadt

Interaktiv ist eine Initiative im Auftrag der Landeshauptstadt München (Kultur/Schule/Soziales) in Verbindung mit dem kommunalen Koordinationsforum Kinder- und Jugendkultur in München (KoFo).

FONDS SOZIOKULTUR
Diese Sonderausgabe „Who's watching you“ wird unterstützt vom Fonds Soziokultur.