Big Brother kommt per E-Mail

Das «Sankt Galler Privacy Interaction Framework» am Beispiel des E-Mail-Trackings erklärt.

Bild:
Fotolia/imacture

Ob bei einer Flugbuchung oder einer Bestellung im Onlineshop: Kaum gibt man seine E-Mail-Adresse an, erhält man regelmässig Nachrichten mit den neuesten Angeboten und Rabattaktionen. So kommt es, dass uns jeden Tag unzählige Werbemails erreichen und das kurze Anschauen und Löschen dieser Nachrichten oft ein Bestandteil unseres Alltags ist. Für viele von uns sind diese Mails ein Ärgernis, weil sie die Aufmerksamkeit von den wichtigen Nachrichten ablenken und wir oft gerade keinen neuen Fernseher, Flug nach Bangkok oder eine Übernachtung am Gardasee benötigen. Aber wussten Sie, dass diese Mails nicht nur den Zweck erfüllen, Sie zu «informieren», sondern dass Sie durch das blosse Öffnen dieser Nachrichten oft auch sehr persönliche Daten über sich preisgeben?

Tracking-Elemente

Fast alle Werbemails enthalten heutzutage sogenannte Tracking-Elemente, mittels derer der Sender viele Informationen über den Empfänger erhält, sobald dieser die Nachricht öffnet. Diese Tracking-Elemente sind als Links oder oftmals als kleine – für den Leser unsichtbare – Bilder in die E-Mails eingebettet. In einer neuen Studie an der Humboldt-Universität Berlin wurden mehr als 600 Werbemails untersucht. 98 Prozent enthielten Tracking-Elemente. Wird die E-Mail geöffnet, erfolgt über einen personalisierten Link ein Zugriff auf einen Server. Dadurch erhält der Sender Informationen darüber, ob, wann, wo und mit welchem Endgerät die E-Mail geöffnet wurde. Durch die Verknüpfung mit Namen und E-Mail-Adresse können so vielfältige Informationen über Sie als Empfänger generiert werden. So können Unternehmen in Erfahrung bringen, wann Sie Ihre E-Mails lesen und wo Sie sich gerade aufhalten.

Diese Praxis wird von einem Grossteil der Unternehmen, die Werbemails versenden, intensiv genutzt. Rechtlich abgesichert werden diese Praktiken durch das Annehmen von Allgemeinen Geschäftsbedingungen oder Cookies durch die Nutzer. Für die Unternehmen können die gewonnenen Informationen ein wertvolles Gut darstellen, das zur zielgerichteten Werbung genutzt oder sogar gehandelt werden kann. Doch ist diese Methode auch legitim und gesellschaftlich akzeptabel? Würden Sie wollen, dass Ihr Reisebüro oder Ihre Lieblingsboutique weiss, wo Sie sich gerade aufhalten und wann Sie in Ihre E-Mails schauen?

Was ist Privatsphäre?

Diese Fragen betreffen alle das grosse Thema der *Privatsphäre im Internet* – oder Online Privacy. Spätestens seit Edward Snowdens Enthüllungen zum NSA-Prism-Programm steht (der scheinbare Verlust von) Online Privacy im Fokus der Öffentlichkeit. Aktuelle Umfragen zeigen, dass sich ein Grossteil der Bürger Sorgen um ihre Privatsphäre im Netz macht. Allerdings ist Privatsphäre ein schwierig zu fassender Begriff. Trotz jahrzehntelanger Forschung gibt es noch keine allgemein gültige Definition, was «privat» genau bedeutet. Geht es dabei um private *Räume*, also die eigenen vier Wände, wo man ganz «man selbst» sein kann? Geht es um einen psychologischen *Zustand* des sich sicher und unbeobachtet Fühlens? Oder geht es um die Kontrolle über persönliche, sensible *Informationen*, wie Handykontakte, sexuelle Präferenzen oder eben den E-Mail-Verkehr?

Verschiedene akademische Disziplinen setzen sich auf unterschiedliche Arten mit dem Phänomen Online Privacy auseinander, von Juristen, Psychologen und Informatikern bis hin zu Philosophen. Meistens haben die einzelnen Disziplinen eine bestimmte Sichtweise, die den Blick auf andere – oft sehr fruchtbare – Zugänge versperrt. Interdisziplinarität ist also gefordert.

Der HSG Privacy Roundtable

Genau diesem Ansatz hat sich eine Initiative von inzwischen acht Doktoranden der HSG verschrieben. Aus verschiedenen Fachrichtungen und Instituten kommend, gründeten sie im Frühjahr 2014 den *Privacy Roundtable* – eine Diskussionsgruppe zum Thema Online Privacy. Aus dem Austausch ist ein Beitrag im Assistierendenband (www.assistierendenband.ch) entstanden, der einen neuen, interdisziplinären Zugang zur Privatsphäre im Internet bietet. Das Autorenkollektiv beschreibt darin das Sankt Galler Privacy Interaction Framework (SG-PIF). Ganz der systemischen Tradition des St. Galler Management-Modells verpflichtet, betrachtet SG-PIF Online Privacy als ein Phänomen, das auf verschiedenen Ebenen beeinflusst wird. Konkret beinhaltet SG-PIF vier Ebenen: individuelle Entscheidungen (mikro), die Rolle von Organisationen (exo), gesellschaftliche Normen und Werte (meso), sowie gesetzliche Rahmenbedingungen (makro). Ein bestimmtes Phänomen, das im Rahmen von Online Privacy auftritt, lässt sich nun mittels Rückgriff auf diese Ebenen präzise und umfassend beschreiben und analysieren. Insbesondere berücksichtigt SG-PIF auch, dass die einzelnen Ebenen sich überschneiden und miteinander interagieren.

Vier Ebenen für ein vollständiges Bild

Untersuchen wir das eingangs beschriebene E-Mail-Tracking durch die Brille des SG-PIF, so wird deutlich, dass wir auch diesen Eingriff in die Privatsphäre nicht vollständig verstehen, wenn wir nur die – in diesem Fall weitestgehend unbewussten – individuellen Entscheidungen (mikro) oder die Strategien von «datenhungrigen» Unternehmen (exo) betrachten. Diese Ebenen sind zweifelsohne wichtig, ein volles Bild erhalten wir aber nur, wenn wir uns auch der gesetzlichen Rahmenbedingungen (makro) bewusst sind, innerhalb derer die anderen Ebenen eingebettet sind. Zudem spielen gesellschaftliche Normen und Werte (meso) eine wichtige Rolle, nicht zuletzt weil Unternehmen auf Vertrauen seitens der Gesellschaft angewiesen sind. Aus dem Zusammenspiel dieser ineinander eingebetteten Ebenen entsteht ein Gesamtbild, welches uns das Phänomen strukturieren und Handlungspotenziale erkennen lässt.

Autorinnen und Autoren: Lea Sophie Aeschlimann, Rehana Harasgama, Flavius Kehr, Christoph Lutz, Veselina Milanova, Severina Müller, Pepe Strathoff, Aurelia Tamò.