Wer ohne Schuld ist

Datenschutz in unserer eigenen EDV

Kaum eine Politgruppe verzichtet heute auf eine Webseite, manche leisten sich Accounts bei Twitter oder gar Facebook, eigentlich alle empfangen E-Mails, nicht selten kommen dazu allerlei Dateien – und wenn es nur Protokolle sind. Fast immer sind dabei personenbezogene Daten im Spiel, nicht selten von Menschen, die mit den Gruppen nichts zu tun haben. Bei einer Fahrrad-Ini mag Achselzucken angesichts gedankenlosen Umgangs mit solchen Daten vielleicht hinzunehmen sein, Ortsgruppen der Roten Hilfe und ihre Bundesorganisation jedoch hantieren etwa bei Unterstützungsfällen oder allgemeiner Beratung mit manchmal sehr heiklen persönlichen Details, wozu im Zweifelsfall schon die Tatsache der Mitgliedschaft gehören kann. Darum müssen wir uns ganz besonders Gedanken über einen verantwortungsvollen Umgang mit den uns anvertratuen Daten machen. Anstöße dazu möchte dieser Artikel liefern.

Zur Einleitung lohnt sich zunächst ein Blick in den bürgerlichen Datenschutz. Dort haben sich in den letzten dreißig Jahren einige Prinzipien herauskristallisiert, die als Mindeststandard auch linken Initiativen gut zu Gesicht stehen. Wesentliche Punkte dabei sind:

Datensparsamkeit oder Erforderlichkeitsprinzip – Daten dürfen nur dann erhoben und gespeichert werden, wenn sie zur Erfüllung einer bestimmten Aufgabe (des „Zwecks“) unverzichtbar sind und dieser Zweck „verhältnismäßig“ gegenüber dem Grundrechtseingriff der Verarbeitung ist. Beispiel: Wenn wir ein PDF von „Was tun wenns brennt“ ins Netz stellen, um Menschen im Umgang mit der Staatsgewalt zu helfen, ist die Speicherung der IP-Adressen der LeserInnen zur Erfüllung dieses Zwecks sicher nicht nötig und damit auch nicht statthaft. *Vielleicht* könnten wir wissen wollen, was für Endgeräte die Leute hatten, mit dem Zweck der gezielten Erstellung darauf optimierter Formate. Der Zweck könnte sogar verhältnismäßig sein, denn die Information „Typ des Endgeräts“ ist im schlimmsten Fall pseudonym, der Grundrechtseingriff also relativ gering.

Zweckbindung – Wenn Daten für einen Zweck erhoben wurden, dürfen sie auch nur für diesen Zweck genutzt werden und müssen gelöscht werden, wenn dieser Zweck erfüllt ist. Aus dieser Forderung ergeben sich regelmäßig auch Fristen, nach denen in jedem Fall gelöscht werden muss. Beispiel: Bei der Bearbeitung von Unterstützungsfällen ist es recht zweifellos sinnvoll, Mailadressen und Telefonnummern der Betroffenen zu haben, weswegen sie gespeichert werden können. Wenn die RH sich aber unter Nutzung dieser Daten bei den Leuten melden würde, um nach Spenden zu fragen, könnten diese mit gutem Recht sauer werden, und um so mehr, wenn das ein paar Jahre nach dem U-Fall passieren würde.

Transparenz – Leute, die uns Daten geben, müssen wissen (können), was mit diesen passiert, was wir sonst noch über sie haben, wann der Kram gelöscht wird, und sie müssen die Möglichkeit haben, sie löschen zu lassen, wenn sie keinen Bock mehr auf uns haben. Für diese Transparenz ist z.B. ein Verfahrensverzeichnis nützlich, in dem zumindest einmal stehen sollte, wer welche Daten von wem wie lange und wozu verarbeitet werden. Nebenbei: Dokumente dieser Art sind übrigens gute Ziele für Anfragen nach Informationsfreiheitsgesetzen.

Warum?

Diese Prinzipien leitet die bürgerliche Gesetzgebung mit einigem Recht direkt aus der Menschenwürde ab (um sie dann regelmäßig zu verletzen, aber das ist dieses Mal nicht das Thema). Auch die Menschenwürde darf mensch wohl getrost als Lightversion von solidarischem Umgang erstmal in den linken Diskurs übernehmen. Bei uns kommt hinzu, dass Daten, die wir haben,

leider nicht immer bei uns bleiben. Die Staatsgewalt beschlagnahmt Rechner oder bricht gleich in sie ein, um unbeobachtet Daten zu klauen, Genoss_innen privatisieren oder verschmeißen die Daten aus Unachtsamkeit, Nazis oder Chefs kommen auf die eine oder andere Weise an sie ran, und plötzlich sind wir schuld an einem Haufen Ärger oder jedenfalls daran, dass Menschen, die sich vertrauensvoll oder mit Hilfsangeboten an uns gewandt haben, bloßgestellt sind.

Also – wer mit personenbezogene Daten in Rechnern verarbeitet, trägt eine erhebliche Verantwortung. Je weniger da schiefgehen kann, desto besser. Dazu gehören natürlich Maßnahmen zur technischen Sicherung der Daten (z.B. Verschlüsselung, Zugriffskontrolle). Die einzig sicheren Daten sind und bleiben aber die, die es gar nicht (mehr) gibt, und diese Sorte Datenschutz kann wirklich niemand unter Hinweis auf fehlende technische Kompetenzen unterlassen.

Das Einfache

Jede Gruppe, die eine Webseite anbietet, geht mit einer recht perfiden Sorte personenbezogener Daten um: IP-Adressen und Header-Daten von Leuten, die die Webseiten lesen oder sonst etwas damit machen. Speziell IP-Adressen sind ganz klar personenbezogen, denn die Staatsgewalt kann sie fast voraussetzungslos für Tage bis Monate konkreten Anschlüssen zuordnen und hat das auch schon in Strafverfahren gemacht („Wer hat dieses Flugblatt hochgeladen?“, „Wer hat alles die Anschlagserklärung gelesen?“ usf). In der Tat dreht sich ein guter Teil der Diskussion über die Vorratsdatenspeicherung exakt um die Auflösbarkeit von IP-Adressen.

Allgemeinere Header-Daten sind zum Beispiel Informationen zum verwendeten Browser („Chrome 4.5, Patchlevel 2304 auf IPhone IOS 3.32, bevorzugte Sprachen Deutsch, Englisch und Esperanto“). Auch sowas kann zur Identifikation von Personen dienen und ist in dem Sinn bedenklich. Sie sind aber weit schwerer aufzulösen und umgekehrt leichter von Nutzer_innenseite zu fälschen (vgl. „Spuren im Speicher“, RHZ 4/10).

Wie bei der Diskussion der Datensparsamkeit schon erwähnt, haben wir eigentlich nie gute Gründe, solche Daten zu speichern; trotzdem tun das fast alle Webserver per Voreinstellung. Wenn ihr euren eigenen Server betreibt, müsst ihr also das Logging per Hand komplett abschalten (oder mindestens die IP-Adressen in den Logs unterdrücken). Schwieriger ist das, wenn ihr „kostenlosen Webspace“ oder gar Schrecklichkeiten wie facebook nutzt – für solche Unternehmen sind Verkehrsdaten Handelsware, und sie zu bitten, doch lieber nichts zu speichern, konstituiert einen Angriff auf ihr Geschäftsmodell. Es hilft in so einem Fall nur ein Wechsel zu Providern aus unseren Strukturen (z.B. jpberlin oder nadir; eventuell gibt es bald ein von RH-Genoss_innen bereitgestelltes System zum Hosting von OG-Inhalten) oder zu Infrastruktur befreundeter Initiativen.

Die Entscheidung, gar nicht zu loggen, ist bei Verwaltungszugängen (ftp, ssh, dav) zunächst nicht ganz so einfach, und zumindest sind dabei normalerweise keine persönlichen Daten Gruppenfremder betoffen. Dazu kommt vielleicht das Bauchgefühl, so im Zweifel rauskriegen zu können „wer es war“, wenn plötzlich blöder Content auf der Seite steht oder es etwa einen Einbruch gab. De facto ist diese Sorte Forensik aber kitzlig und bei halbwegs kompetenten Einbrecher_innen für nichtstaatliche Akteure auch fast aussichtslos. Wer die Möglichkeit hat, sollte also das Speichern von Daten auf diesen Zugängen abdrehen.

Mails

Offensichtlich ist bei Mails eine „gar nicht speichern“-Politik nicht machbar. Zumindest für eine Weile liegen sie auf Servern und allerlei Endgeräten. Damit stellt sich die Frage nach technischen Sicherungen (z.B. Verschlüsselung des Datenträgers; das ist aber mindestens ein eigener Artikel) ebenso wie die nach den Speicherfristen. Klar ist es nett, nach ein paar Monaten noch nachsehen zu können, was wer mal wollte. Und es ist vermutlich durchaus legitim, ein Einverständnis der Absender_innen zu so einer Speicherung zu unterstellen. Aber *irgendwann* sollten die Mails schon verschwinden, z.B. nach Abschluss eines U-Falls oder immer nach einem Jahr; Bonuspunkte gibt es, wenn so eine Politik nicht nur beschlossen, sondern auch publiziert ist.

Doch ist das in der Realität haarig, da Mails meist über Verteiler gehen und also in vielen Mailboxen landen. Manche davon sind auf haarsträubend ungesicherten Rechnern, andere, noch schlimmer, bleiben in Webmail-Konten. Vor allem die „populären“ Webmail-Provider (web.de, gmx, hotmail usf) sind

da fatal, da die Polizei auch nach dem Verfassungsgerichtsurteil zum Telekommunikationsgesetz vom 25.2.2012 noch sehr liberal Passwörter für diese Konten bei den Betreibern erfragen kann und Rechtsprechung existiert, die den Inhalten der Postfächer den Schutz des Telekommunikationsgeheimnisses abspricht.

Ideal wäre hier ein Verfahren, nach dem nur ein Mensch in der Gruppe Mails überhaupt archiviert und dabei die vereinbarte Speicherpolitik auch durchhält, während alle anderen Mails von Dritten „möglichst sofort“ löschen; dazu sollten Mails mit personenbezogenen Daten eher konservativ verteilt werden. Klar ist das weit von jeder Praxis in uns bekannten Gruppen weg, aber wenn sich Gruppen durchringen können, das mal als Plan zu formulieren, ist schon viel gewonnen. Als unmittelbare Maßnahme bietet sich zudem an, keine Accounts auf unpolitischen Freemail-Läden für Arbeit mit personenbezogenen Mails zu verwenden, dies um so mehr, als etwa mit riseup.net oder immerda.ch gute Alternativen aus unserem Spektrum existieren.

Andere Dateien

Im Vergleich zu Mails sind „normale“ Dateien mit personenbezogenen Daten, also etwa Protokolle oder Dokumente zu Unterstützungsfällen, meist harmloser: Sie werden bei weitem nicht so weit gestreut und liegen selten auf öffentlichen Servern – dass sie in Diensten wie dropbox unverschlüsselt nichts verloren haben, sollte sich von selbst verstehen. Auch für sie gilt aber: Technisch sichern (also verschlüsseln) und löschen, wenn sie nicht mehr gebraucht werden. „Nicht mehr gebraucht werden“ braucht hier natürlich ebenso viel Interpretation offen wie bei Mails. Es kommt ja schon mal vor, dass nach einem Jahr eine verlorene Seele nochmal nach einem U-Fall fragt, dass wer wissen will, was vor vier Jahren mal besprochen wurde. Ganz toll wäre natürlich eine Anonymisierung der Daten zur Langzeitarchivierung. So viel Rücksicht auf spätere Historiker_innen ist aber wohl selbst nicht verhältnismäßig. Insofern wäre eine definierte Löschfrist (die noch bequem in Monaten auszudrücken ist) wahrscheinlich am ehesten eine realistische Politik; im Zweifel ist eine Archivierung auf Papier (wiederum mit ordentlicher physikalischer Sicherung) weit unkritischer.

Ein Punkt, der dann noch dazu zu bedenken ist, sind Backups. Diese sind nämlich gleich in drei Richtungen problematisch. Erstens werden sie bei Privatmenschen meist eher unzuverlässig gemacht, also sporadisch und auf alle möglichen Medien („Ich hab mal meine Dokumente auf DVD gebrannt“; „Ich hab hier diesen total praktischen Dienst, der mein Backup ins Netz macht“), die dann gerne mal vergessen werden oder verloren gehen. Dann bleiben Dateien, die „im Original“ gelöscht sind, erstmal oder überhaupt (z.B. bei DVDs) im Backup erhalten. Und schließlich liegt der Fehler nahe, verschlüsselte Partitionen „einfach so“ zu backuppen, was dann technische Sicherungen gleich noch mit unterläuft.

Alle diese Probleme sind lösbar, aber vermutlich ist es in unserem Bereich realistischer, persönliche Daten Dritter einfach gar nicht ins Backup zu nehmen. In den meisten Fällen dürfte der Zweck ihres Schutzes gegen unbeabsichtigten Verlust die Datenschutzproblematik des Backups nicht aufwiegen.

Noch ganz sauber?

Wenn ihr euch jetzt fragt, ob die Autor_innen dieses Artikels noch ganz bei Trost sind: Die Frage ist berechtigt. Auch wir können da nicht den Ersten Stein (Marke Jesus) werfen. Dieser Artikel ist nicht zu verstehen als eine Checkliste für politische Korrektheit. Er soll, gerade angesichts weiter wachsender Begehrlichkeiten der Staatsgewalten auf die Inhalte unserer Festplatten und Flash-Chips, aufzeigen, wo wir hinkommen müssen, und zur Frage anregen, welche Daten wir denn wirklich brauchen und was wir einfach löschen können, ohne dass unsere Arbeit ernsthaft beeinträchtigt wäre.

Wenn jetzt ein paar weniger linke Webseiten IP-Adressen von Interessent_innen speichern, ein paar weniger Anfragen in Repressionsdingen unverschlüsselt bei web.de liegen, ein paar weniger U-Fall-Deckblätter mit alten Notebooks weggeworfen werden, wenn sich schließlich ein paar Gruppen darüber austauschen würden, wie sie mit ihnen anvertrauten personenbezogenen Daten umgehen wollen, dann wäre schon viel gewonnen.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a