GI: Datenschutzfeindliche soziale Netzwerke besser meiden

Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik (GI) warnt mit einer Mitteilung vom 16.01.2013 vor der Nutzung datenschutzfeindlicher sozialer Netzwerke wie Facebook und fordert die

- unverzichtbare Einführung datenschutzfreundlicher Grundeinstellungen: Privacy by Default,
- Übertragbarkeit der Nutzerdaten auf andere Anbieter: Right to portability,
- vollständige Löschung aller gespeicherten Nutzerdaten bei Kündigung: Right to be forgotten.

Soziale Netzwerke werden von Privatpersonen und zunehmend auch von Unternehmen, Behörden, Vereinen und anderen Institutionen genutzt. Sie können, beispielsweise zur Außendarstellung und Werbung im Hinblick auf jüngere potenzielle Mitglieder von Bedeutung sein. Allerdings stellen die aktuellen Sozialen Netzwerke häufig ein komplexes und auch kompliziert zu handhabendes wenig beherrschbares Instrument dar; gerade in Bezug auf den Datenschutz.

Das bekannteste und meistgenutzte soziale Netzwerk ist Facebook mit rund einer Milliarde Nutzerinnen und Nutzern, 24 Millionen davon in Deutschland. Aber gerade Facebook ist aus Sicht des Arbeitskreises derzeit der Anbieter im Markt der sozialen Netzwerke, der sich mit am wenigstem um Belange von Datenschutz, Nutzerschutz und Fairness kümmert.

Folgende gravierende Verstöße gegen das Recht auf informationelle Selbstbestimmung hält GI bei Facebook für besonders bedenklich:

- der als Hotlink automatisierte Like-Button: Beim Aufruf einer Webseite mit Like-Button erfährt Facebook – ohne dass der Benutzer den Like-Button über-haupt benutzt und ohne dass er bei Facebook registriert sein muss – die URL der Webseite, die IP-Adresse des Benutzers sowie weitere Daten.
- Benutzer, die zuvor schon einmal facebook.com besucht haben – insbesondere also alle Facebook-Mitglieder – haben ein von Facebook gesetztes Cookie auf ihrem Rechner, das bei jeder Kontaktaufnahme an Facebook gesendet wird. Das Cookie trägt eine dem Benutzer zugeordnete Kennung, die als Pseudonym des Benutzers fungiert. Somit kann Facebook alle Informationen, die zu ein und demselben Pseudonym gehören, zu einem detaillierten Verhaltensprofil des pseudonymen Benutzers zusammenführen.
- Bei Facebook-Mitgliedern ist allerdings nicht einmal die Pseudonymität gewährleistet: Wenn ein Mitglied sich in einer Facebook-Sitzung befindet, erlaubt die ebenfalls per Cookie übertragene Sitzungskennung eine Aufdeckung des Pseudonyms und damit die Verfolgung der gesamten Surf-Historie des Benutzers.
- der Versuch bei der Datenerfassung mittels Kontakten von (Neu-) Mitgliedern: Meldet sich ein Nutzer bei Facebook an, wird ihm nahegelegt („Finde Deine Kontakte bei Facebook“) seine persönlichen E-Mail-Kontakte für Facebook freizugeben. Diese Informationen nutzt Facebook, um weitere Mitglieder zu werben. Bei Beschwerden verweist Facebook auf die (nur implizit) gegebene Bestätigung – die übermittelnde Nutzer im Regelfall nicht erkennen.
- Auf den gespeicherten 75 Milliarden Fotos werden bisher 450 Millionen identifizierte Personen wiedererkannt, die einer Speicherung gar nicht ausdrücklich zugestimmt haben.
- Die immer wieder und kurzfristig ohne Vorwarnung erfolgende Veränderung der Einstellungen und Voreinstellungen zu Datenschutz und Datenflüssen widerspricht datenschutzrechtlichen Grundsätzen.
- Es fehlt die Möglichkeit, die Daten zu einem anderen Anbieter „mitzunehmen“: Damit sie nicht ‚ewig‘ an einen einzigen Anbieter gebunden sind, müssen Nutzer ihre Daten auf andere Systeme portieren können: Right to portability (nur so lässt sich ein erzwungenes Bleiben bei einem Anbieter vermeiden).
- Mangelnde Bereitschaft im Fall der Account-Kündigung gespeicherte Nutzer-daten (vollständig) zu löschen: Right to be forgotten.
- Immer wieder neue Sicherheitslücken in der Verwaltungssoftware, die entgegen dem Nutzerwillen und der Parametrisierung zur Preisgabe personenbezogener Informationen führen. Neben geeigneten Sicherheitsmaßnahmen muss eine Meldepflicht des Betreibers bei Datenschutzverstößen eingeführt werden.

Der aktuelle Entwurf der EU-Kommission einer ‚Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)‘ setzt diese Forderungen weitgehend um und wird vom Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ daher gerade auch im Hinblick auf eine nutzerfreundliche Regelung bei sozialen Netzwerken nachdrücklich unterstützt.

ThLfDI: Informationsfreiheitsgesetz – Wozu ?

Mit dem Jahreswechsel 2013 verfügt Thüringen über ein neues, den freien Zugang zu behördlichen Informationen und Dokumenten regelndes Gesetz. Das vom Thüringer Landtag verabschiedete Informationsfreiheitsgesetz löst das bisherige seit 2008 geltende Gesetz ab, das im Wesentlichen nur auf das bestehende Bundesgesetz verwies und damit insbesondere für BürgerInnen schwer handhabbar war sowie den Informationszugang nur unzureichend regelte. Mit dem neuen Thüringer Informationsfreiheitsgesetz liegt den BürgerInnen in Thüringen erstmals ein Gesetz vor, das umfänglich sowohl den Anspruch, den Umfang und das Verfahren für den freien Zugang zu Informationen der Verwaltung regelt.

Der Informationszugang über Spezialgesetze, wie zum Beispiel das Datenschutzgesetz für Auskünfte über zur eigenen Person gespeicherte Daten, das Umweltinformationsgesetz für Auskünfte über den Zustand der Umwelt und deren Beeinträchtigung oder das Verbraucherinformationsgesetz für Auskünfte über bestimmte Produkte, bleibt auch weiterhin bestehen. Das Informationsfreiheitsgesetz regelt über diese Gesetze hinaus den freien Zugang zu sämtlichen bei Behörden vorliegenden Informationen und die Voraussetzungen, unter denen diese zugänglich gemacht werden sollen. Das Gesetz vergrößert unter Wahrung schutzwürdiger Belange der öffentlichen Verwaltung und gegebenenfalls betroffener privater Dritter die Transparenz der Verwaltung und verbessert die Möglichkeiten der Kontrolle staatlichen Handelns. Informationsfreiheit fördert somit die demokratische Meinungs- und Willensbildung.

Wie funktioniert das?

Um behördliche Informationen zu erhalten oder Einsicht in behördliche Dokumente zu erhalten, ist ein Antrag an die Behörde zu richten, von der die Informationen begehrt werden. Der Antrag kann schriftlich oder mündlich erfolgen. Auch eine elektro-nische Übermittlung, bspw. per E-Mail, ist möglich. Eine Begründung des Antrages ist zwar regelmäßig nicht erforderlich, allerdings muss