OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

Überwachung braucht Transparenz und demokratische Kontrolle

Stellungnahme des OCG Forum Privacy zu den von Edward Snowden aufgedeckten weltweiten Überwachungspraktiken

Das Internet vergisst nicht. Die meisten unserer Aktivitäten hinterlassen heute digitale Spuren: Smartphones verraten unseren Aufenthaltsort, Surfen und Suchanfragen enthüllen unsere Interessen. Die Informationstechnologie hat einen Entwicklungstand erreicht, der es ermöglicht, diese Aktivitäten und die Kommunikation aller Bürgerinnen und Bürger gleichzeitig und nahezu flächendeckend zu überwachen und auszuwerten. Edward Snowdens Enthüllungen über die umfangreichsten Überwachungsaktivitäten in der Geschichte der Menschheit[1] zeigen auf, dass es für den Fortbestand unserer demokratischen Gesellschaftsordnung unerlässlich ist, einen Weg zu finden, mit diesen technischen Möglichkeiten verantwortungsbewusst umzugehen und deren Einsatz wieder unter demokratische Kontrolle zu bringen.

Werden die vorhandenen technologischen Möglichkeiten ausufernd und unabhängig davon, ob ein konkreter Verdacht besteht, zur flächendeckenden Überwachung nahezu aller Bürgerinnen und Bürger eingesetzt, ist dies als Missbrauch dieser Technologien, als Missbrauch der Informatik zu werten. Das Forum Privacy der Österreichischen Computer Gesellschaft (OCG) spricht sich entschieden gegen diesen Missbrauch aus und fordert einen verantwortungsbewussten Umgang mit Informationstechnologie unter Wahrung der Grundrechte auf Privatsphäre und Datenschutz. Öffentlichkeitsarbeit und Bildungsmaßnahmen auf allen Ebenen, die über Datenmissbrauch und betroffene Grundrechte aufklären, sind dafür im Sinne der Entwicklung einer „digitalen Zivilgesellschaft“ eine entscheidende Voraussetzung.

Die Überwachung von verdächtigen Personen kann im Einzelfall entscheidend zur Verhinderung oder Aufklärung von Verbrechen beitragen. Doch die Überwachung aller mit dem Ziel, ein möglicherweise verdächtiges Verhalten festzustellen bzw. vorherzusagen, ist abzulehnen. Das Bewusstsein permanenter Überwachung und Kontrolle führt dazu, dass die Menschen selbst legitimes Verhalten verändern und mit opportunen Anpassungen an vermeintliche Erwartungshaltungen reagieren. Die Rechte auf freie Meinungsäußerung und informationelle Selbstbestimmung werden dadurch unverhältnismäßig eingeschränkt, was auch den politischen Diskurs und somit die politische Partizipation der Bevölkerung beeinträchtigt – selbst ohne bewusste Kontrolle politisch Andersdenkender mittels der vorhandenen Überwachungstechnologien.[2] Diese Kontrolle und andere Missbrauchsrisiken zählen ebenfalls zu den Gefahren der Überwachung der Bevölkerung und der Speicherung großer Mengen personenbezogener Daten.

[1] Überblick über die Fakten zu den Enthüllungen: http://www.zeit.de/digital/datenschutz/2013-07/faq-nsa-skandal/komplettansicht

[2] Die Beispiele dafür, dass dies nicht nur in autoritären Regimen vorkommt, reichen vom Watergate-Skandal bis in die jüngere Geschichte und auch nach Österreich.

Zudem führen Überwachungsmaßnahmen unweigerlich zu falschen Verdächtigungen: Algorithmen sind niemals fehlerfrei, die „verdächtigen" Handlungen sind oft alltäglich und banal. Zahlreiche Fälle der vergangenen Jahre zeigen, dass zu Unrecht erfolgte Verdächtigungen für die Betroffenen folgenschwer sein können. Nicht nur dieser Umstand widerlegt die Aussage, „wer nichts zu verbergen hat, hat nichts zu befürchten."

Selbst wenn ein Algorithmus zur Identifikation „verdächtigen Verhaltens" so gut arbeitet, dass er nur in einem von einer Million Fälle harmloses Verhalten fälschlicherweise für verdächtig hält, führt dies alleine im Zuge der Analyse der elektronischen Aktivitäten aller Österreicherinnen und Österreicher täglich zu zahlreichen falschen Verdächtigungen. Jene, die etwas Kriminelles zu verbergen haben, werden zudem immer Möglichkeiten finden, sich vor Überwachung wirksam zu schützen.

Weder ungeheurer Überwachungsaufwand noch andere Maßnahmen können hundertprozentige Sicherheit gewährleisten. Schon allein aus diesem Grund muss eine Balance zwischen Sicherheit und Privatsphäre gefunden werden.

Das OCG Forum Privacy fordert daher:

- **Transparenz und demokratische Kontrolle**: Demokratische Staaten müssen ihre Überwachungsmaßnahmen offenlegen und dazu bereit sein, diese Maßnahmen von Informatikern, Juristen, Soziologen etc. evaluieren zu lassen; dies sollte in eine öffentliche Debatte über die Befugnisse der Sicherheitsbehörden und Geheimdienste münden.
- **Offenlegung:** Die österreichische Bundesregierung muss völkerrechtliche Vereinbarungen Österreichs mit den USA und anderen Staaten, die teilweise bis weit in die Zeit des Kalten Krieges zurückreichen, offenlegen und glaubhaft die Vermutung ausräumen, dass ihre Reaktionen auf die Enthüllungen rund um PRISM deswegen so zurückhaltend ausfielen, weil sie von diesen Aktivitäten wusste und auch österreichische Behörden davon profitieren.
- **Datenschutz**: Eine wirksame Nachfolgeregelung für das Safe-Harbor-Abkommen muss verhandelt und abgeschlossen werden, um das europäisches Datenschutzniveau für in die USA übertragene Daten zu gewährleisten. Das gegenwärtige Abkommen erfüllt diesen Zweck nur unzureichend. Auch EU-Kommissarin Reding spricht von Safe Harbor als „Schlupfloch".[3]
- **Grundrechte**: Eine völkerrechtliche Vereinbarung zur Wahrung der Grundrechte im Internet und zur Kontrolle des Cyberwar muss verhandelt und abgeschlossen werden.
- **Europäische Cloud:** Die Förderung einer europäischen Cloud („Airbus in the Clouds"): Es müssen Initiativen gestartet werden, um zu erreichen, dass in Zukunft die wichtigsten Dienstleistungen im Internet auch von konkurrenzfähigen europäischen Unternehmen angeboten werden. Dadurch sollen nicht nur Monopole ausgeschaltet und die europäische Wirtschaft durch Nutzung ihrer spezifischen Standortvorteile gestärkt, sondern vor allem den Bürgerinnen und Bürgern (aller Staaten) Dienste zur Verfügung gestellt werden, die ihre Privatsphäre respektieren und nicht von Behörden zur unverhältnismäßigen Herausgabe von Nutzerdaten gezwungen werden können. Dies ist dringend nötig, wie die Fälle der E-Mail-

[3] http://europa.eu/rapid/press-release_MEMO-13-710_en.htm

Anbieter Lavabit[4] und Silent Circle[5] zeigen, die unter dem Druck der US-Behörden von ihren Betreibern freiwillig geschlossen wurden (genaueres durften die Betreiber dazu nicht bekannt geben).

- **Evaluation:** Die in der österreichischen Verwaltung eingesetzten Softwareprodukte und IT-Services müssen hinsichtlich deren Sicherheit gegenüber Überwachungsmaßnahmen evaluiert werden.[6]
- **Spionage:** Ermittlungen und diplomatische Schritte sind einzuleiten, um Wirtschaftsspionage mittels staatlicher Überwachungsmaßnahmen zu unterbinden.[7]
- **Pressefreiheit:** Die Achtung der Freiheit der Presse: Dieses Grundrecht gilt auch und insbesondere für jene Journalistinnen und Journalisten, die unverhältnismäßige Überwachungsmaßnahmen bekannt machen und dadurch entscheidend dazu beitragen, die Überwachung wieder unter demokratische Kontrolle zu bringen.

Gezeichnet von den Mitgliedern des Forum Privacy der Österreichischen Computer Gesellschaft (OCG):

Walter Hötzendorfer, Co-Leiter
Dr. Christof Tschohl, Co-Leiter
Reinhard Goebl, Präsident der OCG
Dr. Georg Becker
tit. ao. Univ.-Prof. Dr. Gunter Ertl
ao. Univ.-Prof. Dr. Gerald Futschek
O. Univ.-Prof. Dr. Georg Gottlob
Wolfgang Keck
Dr. Wolfram Proksch
ao. Univ.-Prof. DDr. Erich Schweighofer
Univ.-Prof. Dr. Hannes Werthner

Bei einer Veröffentlichung in digitaler Form sollte auch auf dieses hervorragende Video verlinkt werden: http://www.youtube.com/watch?v=iHlzsURb0WI

[4] http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/ Lavabit war auch von Edward Snowden verwendet worden.
[5] http://www.forbes.com/sites/parmyolson/2013/08/09/e-mails-big-privacy-problem-qa-with-silent-circle-co-founder-phil-zimmermann/
[6] Es ist darauf hinzuweisen, dass grundsätzlich nur Open-Source-Software umfassend auf das Vorhandensein von sogenannten Backdoors untersucht werden kann.
[7] Hinweise auf Wirtschaftsspionage: http://www.washingtonpost.com/politics/kerry-to-face-questions-on-nsa-spying-during-south-america-trip/2013/08/12/afdab47e-0382-11e3-88d6-d5795fab4637_story.html