Rüdiger Weis

Kryptographie, Open Source und Gesellschaft

Wer sich gegen die allumfassende Internet-Überwachung zur Wehr setzen möchte, greift schon länger auf eine starke Verschlüsselung von Daten (Kryptographie) und Open Source Software zurück. Jedoch belegen die von Edward Snowden veröffentlichten Dokumente, dass die mit Kryptographie zu erzielende Sicherheit trügt. Zahlreiche Verschlüsselungstechniken, ja selbst die mathematischen Grundlagen dieser Verfahren wurden kompromittiert bzw. manipuliert. Rüdiger Weis zeigt im folgenden Beitrag, welche Anforderungen an Verschlüsselungsverfahren zu erfüllen sind, damit diese als hinreichend sicher angesehen werden können. Zugleich warnt er davor, Sicherheit allein mit technischen Mitteln erreichen zu wollen. Seine Kernthese: Es gibt keinen absoluten Schutz für einmal gespeicherte Daten. Datensparsamkeit, also besonders sensible Daten überhaupt nicht zu erfassen oder zu speichern, ebenso wie ein stärkerer rechtlicher Datenschutz sind für ihn deshalb unerlässlich, um die Integrität von IT-Systemen wiederzugewinnen.

Die weltweite elektronische Vernetzung stellt wohl eine der tiefgreifendsten Veränderung seit der industriellen Revolution dar. Das gesellschaftliche Zusammenleben, unser gesamtes Wirtschaftsleben, das Verhältnis zwischen Bürger und Staat und das Verhältnis der Staaten untereinander stehen vor tiefgreifenden Herausforderungen. Wer hier von „Neuland“ spricht, liegt vielleicht gar nicht so falsch, wie oberflächlichere Kommentatoren meinen. Oft wird in der Diskussion das technikfixierte „code is law“ vorgebracht, und in der Tat scheint die Gesetzgebung technischen Entwicklungen fast nur noch hinterherzulaufen. Allerdings ist es ja aber gerade das Wesen einer freiheitlichen Gesellschaft, dass der Staat Innovation nicht behindern, sondern einen fairen Rechtsrahmen vorgeben sollte. Hierbei kann Technik der Politik gerade dort helfen, wo sich Diplomatie allein als machtlos erwiesen hat. Die Regierungen weltweit sind daran gescheitert, das flächendeckende Abhören von Bürgern und Industrie zu verhindern. Freie Software und starke Kryptographie kann dies. Und auch darüber hinaus sind Kryptographie und Open Source Software mächtige Werkzeuge, um die digitale Gesellschaft freiheitlich und demokratisch zu gestalten.

Das Internet bietet die Möglichkeit der einfachen Teilhabe. Jeder kann sich umfassend aus nichtstaatlichen Quellen informieren und auch die aktive Teilnahme am politischen Meinungsbildungsprozess ist dank sozialer Netze und des einfachen Publi-

zierens mittels Blogs und Podcasts sehr niedrigschwellig möglich geworden. Andererseits wurde schon von Anfang an von der Wissenschaft gewarnt, dass im Internet schon konstruktionsbedingt eine allumfassende Überwachung möglich ist. Nach Snowden ist es unstrittig, dass Staaten diese Überwachung durchführen.

„Crypto works“

Die gute Nachricht ist, dass wissenschaftlich starke Kryptographie auch für übermächtige Geheimdienste nicht brechbar sein dürfte. „Crypto works. It’s not an arcane black art. It is a basic protection, the Defense Against the Dark Arts for the digital world. We must implement it, actively research it“, so Edward Snowden im Guardian vom 11. März 2014.

Kryptographie geht bereits bei der wissenschaftlichen Modellbildung von einem fast allmächtigen Gegner aus. Der Angreifer kann alle Nachrichten lesen und übertragene Nachrichten ändern. Die einzige Voraussetzung auf Verteidigerseite ist das sichere Erzeugen und Speichern von wenigen Bits für die kryptographischen Schlüssel. Nach Snowden wissen wir genauer, an welchen Kabelstellen abgehört wird und auf den Cent genau, wie viel Geld für Kryptoangriffe vorhanden ist – nicht uninteressant, aber wissenschaftlich betrachtet nur eine Fußnote. Die „übertriebene Paranoia“ der Theoretiker hat sich also mal wieder als die realistischste Einschätzung der praktischen Bedrohungslage erwiesen. Kryptographie ermöglicht durch Mathematik auf einer kleinerfingernagelgroßen Fläche oder mit einer handvoll Programmzeilen, Daten sicher selbst gegen eine weltweite Geheimdienstzusammenarbeit zu verschlüsseln. Freie Software ermöglicht dies kosten- und hintertürenfrei.

Pessimisten meinen, dass Kryptographie die letzte Brandmauer gegen eine umfassende Überwachung darstellen könnte, die allerdings in der Praxis häufig umgangen werden kann. Optimisten glauben, dass Kryptographie zu einer Stärkung des Einzelnen gegenüber den Staaten führt und damit eine Schlüsseltechnologie für eine freiheitlich, demokratische Gestaltung des digitalen Lebensraumes darstellt. „Trust the math. Encryption is your friend.", so Bruce Schneier im Guardian vom 6. September 2013.

Allerdings sollten zukünftig Warnungen aus der Wissenschaft vor schwacher Kryptographie ernst genommen werden. Starke Kryptographie sollte als Standardeinstellung benutzt und im klugen Ingenieursinne ausreichend große Sicherheitsspielräume, sprich bewährte Algorithmen mit langen Schlüssellängen, gewählt werden. Nach Snowden ist es sicher, dass kryptographische Verfahren, gegen die wissenschaftliche Vorbehalte bestanden, wohl auch praktisch gegen mit Milliarden ausgestattete Gegnern mehr als problematisch sind.

Mathematischer Forschungsbedarf bei Elliptischen Kurven

Zentraler Baustein für die Sicherheit von elektronischer Kommunikation ist die Verwendung von kryptographischen Verfahren mit öffentlichen Schlüsseln. Diese werden sowohl für die Verschlüsselung, als auch für die Authentifizierung verwendet. Hierfür halten Kryptographen schon seit vielen Jahren Standardverfahren mit einer Schlüssellänge von 1024 bit für brechbar. Die staatlichen Stellen verpflichten schon seit längerem auf eine Mindestlänge von 2048 bit, wie sie beispielsweise Windows 8 verwendet und halten längere Schlüssellängen schon mittelfristig für empfehlenswert.

Viele Kryptographieforschern empfehlen mindestens 4096 bit. Wegen dieser Anforderungen diskutieren viele Wissenschaftlern die Verwendung von Elliptischen Kurven Kryptosystemen. Die Hauptidee hierbei ist, das schon lange bekannte Diskrete Logarithmus Problem (DLP) auf mathematisch anspruchsvollen Strukturen zu verwenden. Die Mehrheit der kryptographischen Forschung ist der Ansicht, dass ECC ähnliche Sicherheit liefert wie RSA und dies bei deutlich kürzeren Schlüsseln und besserer Geschwindigkeit. Diese Eigenschaften sind besonders im Bereich Smartcards und eingebetteten Systeme bedeutend.

Allerdings mehren sich seit geraumer Zeit die Zweifel, ob wirklich gleiche Sicherheit mit deutlich geringerem Zeit und Speicheraufwand zu realisieren ist. Die Annahmen, die dieser Einschätzung zu Grunde liegen, sind sehr weitreichend. Eine Minderheit der Kryptographen kritisiert, dass man sicher lediglich weiß, dass der gegen DLP Systeme über endlichen Körpern wirkungsvolle Index-Calculus Angriff nicht unmittelbar gegen das DLP über der additiven Gruppe von Elliptischen Kurven angewendet werden kann. Hieraus zu folgern, dass nur Standardangriffe anwendbar sind, ist eine durchaus kritisch zu sehende Annahme. Diese Standardangriffe sind universell einsetzbar und nutzen keinerlei Optimierungen der zu Grunde liegenden mathematischen Strukturen. Gerade die reichhaltige algebraische Struktur von Elliptischen Kurven könnte jedoch überraschende und sehr wirkungsvolle Angriffe möglich machen. Zudem ist ECC wegen der kürzeren Schlüssellänge viel anfälliger gegen Angriffe mit Quantencomputern (Shor Algorithmus). Nach Snowden wissen wir auf den Cent genau, dass die NSA erhebliche Mittel in die Forschung zu Quantencomputern steckt.

Ein erhebliches praktisches Problem stellt weiterhin die Tatsache dar, dass ECC-Systeme eine Reihe von mathematisch höchst sensiblen Parametern benötigen. So wurde von offen forschenden Kryptographen in einem NIST-Standard schon im Juni 2006 die hohe Wahrscheinlichkeit einer Manipulation von Elliptischen Kurven bei Parametern für einen Zufallsgenerator (Dual Elliptic Curve Deterministic Random Bit Generator) aufgedeckt. Nach Snowden bestätigt sich die Existenz einer NSA-Backdoor in einem NIST Standard. Der Vertrauensverlust der Standardisierungsbehörde ist ein harter Schlag für die Informatik. Die von NIST und NSA vorgeschlagenen Elliptischen Kurven müssen daher offensichtlich wissenschaftlich nochmals gründlich untersucht werden.

Starke Kryptographie als Standard-Einstellung

Die Enthüllung zum Behördenvorgehen gegen den Mail-Anbieter Lavabit zeigen, wie riskant kryptographisch problematische Einstellungen sind. Bei der Nutzung der bisherigen Standardeinstellungen bedeutet die erzwungene Herausgabe von SSL-Schlüsseln die automatische Kompromittierung der gesamten, sicherlich von der NSA aufgezeichneten Kommunikation *aller* Kunden.

Der getroffene Mail-Anbieter Lavabit beendete den Geschäftsbetrieb, Kommentatoren schrieben über das „Todesurteil für US-Kryptographie" und für US-Cloudanbieter könnten diese rechtlichen Probleme in der Tat das Aus vieler Geschäftsbereiche bedeuten. Und auch hier ist dank kryptographischer Forschung die Lösung nur einen Maus-Klick entfernt. Perfect Forward Secrecy (PFS) ermöglicht, dass durch eine Kompromittierung eines SSL-Serverschlüssels nicht die gesamte Kommunikation von Unschuldigen betroffen ist. Nach Snowden sollten 1024 bit Schlüssel und RC4 nicht mehr verwendet und die Schlüsselvereinbarung auf Perfect Forward Secrecy umgestellt werden.

Warnung vor Windows 8/10

Neu bewertet werden muss die Initiative von Microsoft, bei der Einführung von Windows 8/10 den Nutzern eine neue, von Microsoft kontrollierte Sicherheitsarchitektur aufzuzwingen. Hierbei soll ein Trusted Computing Modul (TPM) in die persönlichen Computer und Mobilgeräte eingebaut werden. Dieses enthält einen Schlüssel auf den der/die Besitzer_in des Computer keinen Zugriffs hat. Zusammen mit den nun von Microsoft implementierten Verfahren innerhalb von Windows 8/10 (insbesondere Secure Boot) wird den Nutzern weitgehend die Kontrolle über ihre eigene Hardware und Software entzogen.

Ähnlich analysierte das Bundesamt für die Sicherheit in der Informationstechnik in einer „Stellungnahme des BSI zur aktuellen Berichterstattung zu MS Windows 8 und TPM":

> *„Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher. Daraus ergeben sich für die Anwender, speziell auch für die Bundesverwaltung und kritische Infrastrukturen, neue Risiken."*[1]

Es erinnert fatal an eine elektronische Fußfessel. So kann beispielsweise über das Netz angefragt werden, ob nur genehmigte Software läuft – das Ende der persönlichen Computer und Smartphones.

Kryptographen warnen vor Trusted Computing

Whitfield Diffie, einer der Entdecker der Public-Key-Kryptographie, zeigte sich besorgt über die dominierende Stellung von Microsoft und forderte, dass die Benutzer die vollständige Kontrolle über die Schlüssel des eigenen Computers behalten sollten:

> *„(The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer. (...) To risk sloganeering, I say you need to hold the keys to your own computer." (zitiert nach EETimes, 15. April 2003)*

Auch Ron Rivest mahnte eindringlich, die möglichen Konsequenzen gründlich abzuwägen:

> *„We should be watching this to make sure there are the proper levels of support we really do want. (...) We need to understand the full implications of this architecture. This stuff may slip quietly on to people's desktops, but I suspect it will be more a case of a lot of debate." (zitiert nach EETimes, 15. April 2003).*

Wenn Wirtschaft und Behörden mittels Windows und Trusted Computing eine Sicherheitsinfrastruktur aufbauen, können die US-Behörden im Zweifelsfall die völlige Kontrolle übernehmen.

> *„Darüber hinaus können die neu eingesetzten Mechanismen auch für Sabotageakte Dritter genutzt werden. Diesen Risiken muss begegnet werden." (BSI, August 2013, a.a.O.).*

Angesichts der Tatsache, dass wiederholt Druck auf Herstellern ausgeübt wurde, Hintertüren einzubauen, wirkt die Idee, dass ein Schlüssel vom/von der Benutzer_in nicht ersetzt werden kann, sehr bedrohlich. Besonders brisant ist, dass die geheimen Schlüssel während des Herstellungsprozesses außerhalb des Chips erzeugt und danach in den Chip übertragen werden. Hier ist es trivial, eine Kopie aller Schlüssel herzustellen. Es ist nicht auszuschließen, dass entsprechende Rechtsvorschriften bestehen und über diese nicht berichtet werden darf. Ein anderes realistisches Szenario, dass der TPM Hersteller nicht in der Reichweite der NSA sondern beispielsweise in der Volksrepublik China sitzt, kann nicht wirklich beruhigen.

Da neben den Überwachungsmöglichkeiten auch die Wahlmöglichkeiten der Nutzer eingeschränkt werden, stellen sich natürlich kartell- und verbraucherrechtliche Fragen. Unter anderem die Tatsache, dass Microsoft die übliche Praxis verlassen hat und den Überwachungschip automatisch einschaltet und sich bei vielen Systemen

selbst nicht mehr ausschalten lässt, verstößt unter anderem gegen das Eckpunktepapier des Bundesinnenministeriums zur vertrauenswürdigen Technikgestaltung.

Secure Boot Probleme für Linux

Nachdem die Einführung einer Microsoft kontrollierten Sicherheitsinfrastruktur durch politischen Widerstand lange aufgehalten werden konnte, hat Microsoft ein weiteres Mal in Geheimverhandlungen Fakten geschaffen. In den Hardwareanforderungen für Windows 10 wird Secure Boot verpflichtend vorausgesetzt. Alternative Betriebssysteme können in der Praxis bisher nur mit technisch und rechtlich nicht unproblematischen Notkonstruktionen gestartet werden.

Microsoft kann und hat auch ohne nachvollziehbare Begründung konkurrierende Bootloader deaktiviert. Ein Szenario, dass Microsoft (möglicherweise durch US Regierungsdruck) die Berechtigung für die von Microsoft unterschriebenen Bootloader für Linux-Distributionen zurückzieht, will man sich insbesondere für sicherheitskritische Systeme oder eingebettete Systeme nicht wirklich vorstellen.

> *„Insbesondere können auf einer Hardware, die mit einem TPM 2.0 betrieben wird, mit Windows 8 durch unbeabsichtigte Fehler des Hardware- oder Betriebssystemherstellers, aber auch des Eigentümers des IT-Systems Fehlerzustände entstehen, die einen weiteren Betrieb des Systems verhindern. Dies kann soweit führen, dass im Fehlerfall neben dem Betriebssystem auch die eingesetzte Hardware dauerhaft nicht mehr einsetzbar ist. Eine solche Situation wäre weder für die Bundesverwaltung noch für andere Anwender akzeptabel.“ (BSI, August 2013, a.a.O.).*

Während deutsche Behörden darüber diskutieren, wie sehr vor Windows 8 gewarnt werden sollte, verbot die Volksrepublik China Windows 8 auf staatlichen Computern.

Alternative Vertrauensanker

Es erscheint zwingend notwendig, Alternativen zum Vertrauensanker von Microsoft zur Verfügung zu stellen. Aus technischen Gründen ist dies sogar deswegen notwendig, weil Microsoft mit einer Schlüssellänge von 2048 bit arbeitet, welche vom BSI nicht für langfristige Sicherheit empfohlen wird.

Für den staatlichen Bereich könnte beispielsweise die Bundesnetzagentur eine führende Position einnehmen. Hier sind im Zusammenhang mit dem Signaturgesetz schon erhebliche Vorarbeiten vorgenommen worden. Für nichtstaatliche Bereiche erscheint eine gemeinnützige Stiftung außerhalb der USA die bessere Lösung. Ähnliche Diskussionen werden bereits zu ICAN und DNSSEC Rootzonen-Schlüssel geführt.

Die Kryptographieforschung hat Lösungen für feingranulare Sicherheitspolitiken mit mathematisch beweisbaren Sicherheitseigenschaften entwickelt. Beispielsweise können Vertrauensbeziehungen durch mehre mögliche Stellen dezentralisiert werden oder eine Zusammenarbeit von mehren Instanzen erforderlich gemacht werden.

Hintertüren in Closed Source Soft- und Hardware

Wenn die geheimen Schlüsselinformationen durch Hintertüren übertragen werden, kann natürlich die stärkste Kryptographie nichts ausrichten. Die bestätigten geheimen Einbauten von Hintertüren durch US Firmen führen ein weiteres Mal die Notwendigkeit für eine neue Vertrauensbasis für die digitale Welt vor Augen. Hierfür sind Schlüsselkontrolle durch die Anwender, nachvollziehbare Standardisierungsprozesse und einsehbarer Sourcecode für Software und Hardware als unabdingbar anzusehen. Nach Snowden ist bekannt, dass die Geheimdienste über einen Milliarden-Etat verfügen, um die Sicherheit von kommerzieller Software und Geräte mit Hintertüren zu versehen. Lesbarer Quellcode und aufmerksame Entwicklern bieten hiergegen Sicherheit.

Lesbarer Quellcode

Während die über die Notwendigkeit der ausschließlichen Verwendung von Open Source Programmen für sicherheitskritische Bereiche noch kontrovers diskutiert wird, ist die schwächere "Lesbarer Quellcode"-Forderung innerhalb der Wissenschaftsgemeinde unumstritten. Ohne die Möglichkeit, den Quellcode zu überprüfen, ist es faktisch unmöglich, Hintertüren zu entdecken.

Lesbarer Quellcode bedeutet nicht zwangsläufig die Verwendung einer offenen Lizenz. Auch veröffentlichter Quellcode kann unter kommerzielle Lizenzen gestellt werden, die die Verwendung und Weitergabe nahezu beliebig einschränken können. Dies ist seit langem gängige Praxis, wie die Beispiele PGP und CryptoPhone zeigen.

Shared Code Probleme

Shared Code Initiativen für Windows, die beispielsweise Microsoft mit verschiedenen Regierungen vereinbart haben, bieten geringeren Schutz, da nicht die gesamte kryptographische Forschungsgemeinde an der Sicherheitsanalyse teilnehmen kann. Ein exklusiver Quellcode-Zugang für Regierungen ist jedoch problematisch, da viele Dienste diesen Wissensvorsprung für Angriffe missbrauchen.

Open Source kann Sicherheitslücken schneller schließen

Open Source Programme bieten den wichtigen Vorteil, dass beim Schließen von Sicherheitslücken nicht auf die Herstellern gewartet werden muss. Die Zeit zwischen der Veröffentlichung einer Sicherheitslücke und dem Schließen dieser durch die Herstellern ist unstrittig die Zeit der höchsten Gefährdung. In der Praxis sind derartige Hochrisikozeiten von mehreren Monaten nicht unüblich. Jedoch zeigen Sicherheitskatastrophen, wie beispielsweise in der systemrelevanten Open-SSL Implementierung, dass auch im Open Source Bereich ein erheblicher Handlungsbedarf besteht. Da auch staatliche Stellen häufig Open Source Lösungen einsetzen und damit selbst nach konservativen Schätzungen Milliardeneinsparungen realisieren, besteht wegen der Sorgfaltspflicht eine staatliche Verpflichtung, hier für eine Grundsicherheit zu sorgen.

Staatsaufgabe Sicherheit in der Informationstechnik

Die politische und juristische Frage, ob Regierungen Cyberangriffswaffen („Bundes-Trojaner“) zum Schutze hoher Rechtsgüter entwickeln dürfen, oder dies verfassungsrechtlich unakzeptabel ist, wie ein entsprechendes Urteil des Bundesverfassungsgericht nahe legt, soll an dieser Stelle nicht diskutiert werden. Aus informatischer Sicht muss jedoch in diesem Fall auf technische und organisatorische Probleme hingewiesen werden, die beispielsweise bei der Einblickgewährung in den Windows-Quellcode auftreten. Die Kenntnis des Quellcodes erleichtert es Angreifern ganz erheblich, ausnutzbare Schwachstellen zu finden. Hier haben staatliche Stellen, die neben dem Schutz der Anwendern auch aktive Angriffe entwickeln, einen nicht auflösbaren Zielkonflikt. Aus diesem Grunde sollten staatliche Stellen die digitale Verteidigung von Bürgern und Wirtschaft organisatorisch strikt von der Entwicklung von Cyberangriffswaffen trennen.

Die Bundesregierungen haben diesen Punkt schon recht früh durch die Gründung des Bundesamtes für Sicherheit in der Informationstechnik teilweise adressiert. Hier erscheint es sinnvoll, eine weitere organisatorische Stärkung, etwa durch die Konstitution einer eigenen Bundesbehörde, umzusetzen. Diese könnte sich etwa an den Reformvorschlägen der Bundesdatenschutzbeauftragten Andrea Voßhoff zur organisatorischen Ausgestaltung und Stärkung der Unabhängigkeit des Bundesdatenschutzbeauftragten oder dem seit 2000 bestehenden Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein anlehnen.

Eine unabhängige Bundesbehörde für die Sicherheit in der Informationstechnik könnte, wie bereits seit Jahrzehnten der Datenschutz, eine deutsche Pionierleistung für eine freiheitlich demokratische Gestaltung des Internets darstellen.

Datensparsamkeit als Querschnittsaufgabe

Beginnend mit dem Volkszählungsurteil des Bundesverfassungsgerichts hat sich in Deutschland ein weltweit beachtetes Datenschutzrecht in Gesetzgebung und Rechtsprechung entwickelt. Datensparsamkeit ist die verfassungsrechtlich und höchstrichterlich geforderte einzuhaltende Norm. Die Tatsache, dass gespeicherte Daten in der real existierenden IT-Welt nicht gesichert werden können, macht Datensparsamkeit zur Querschnittsaufgabe.

Bedeutend für eine gesellschaftliche Einschätzung ist auch die Tatsache, dass neben den Diensten fremder Staaten, auch Privatpersonen und Firmen in der Praxis recht einfach (in der Regel rechtswidrigen) Zugriff auf die heutigen Computersystemen erlangen können. Es haben sich hier Online Marktplätze für ausnutzbare Sicherheitslücken (Zero-Days) gebildet, an denen sich in rechtlich problematischer Weise auch deutsche Dienste beteiligen. Die Preise sind schwankend, allerdings meist für höhere Einkommen und kleinere Firmen durchaus finanzierbar.

Heute müssen sich Datenschutzexperten daher auch in hochkonfliktäre Diskussionen einbringen. Das hier leider vorherrschende politische Diskussionsklima schreckt dabei verständlicher Weise viele Wissenschaftlern ab. Dennoch gebietet es die gesellschaftliche Verantwortung, darauf hinzuweisen, wenn technische Entwicklungen, wie eine allumfassende Überwachung oder die praktische Angreifbarkeit von Computersystemen, juristische Datenschutzzusicherungen praktisch unwirksam werden lassen. In der Computersicherheitsforschung herrscht die Meinung vor, dass Daten auf vernetzten Computersystemen generell als hackbar anzusehen sind. Wenn das nicht vorgesehene Veröffentlichen von Daten zu nicht akzeptablen Problemen führt, dürfen Daten nicht gespeichert werden.

Daten von besonders gefährdeten Personengruppen

Bei einer Abwägung von Datenspeicherung ist neben der rechtlichen Sicherung von Daten gegen Zugriffe, die Auswirkungen von einer rechtswidrigen Veröffentlichung auf die Betroffenen in besonderer Weise zu berücksichtigen. Beispielsweise wurde in der Diskussion über eine Änderung des Prostitutionsgesetzes eine Pflichtregistrierung von Sexarbeiterinnen und Sexarbeitern gefordert. Dieses Vorgehen wurde von Frauenrechtlerinnen, Sozialorganisationen und Datenschützern heftig kritisiert. Von den Berufsvertreterinnen wurde in diesem Zusammenhang neben der Sorge vor staatlicher Diskriminierung (z. B. wie in Schweden) und gesellschaftlicher Ächtung durch religiösen oder politischen Fanatismus (z. B. Schwarzer-Kampagne), auch auf eine erhöhte Gefahr für Leib und Leben durch Triebtätern hingewiesen.

Während die beiden ersten Punkte Teil einer verbittert geführten Diskussion sind, auf die hier nicht näher eingegangen werden soll, ist es unstrittig, dass angesichts der erhöhten Gefährdung der zugesicherte juristische Datenschutz in keiner Weise als ausreichend angesehen werden kann (vergleiche auch Stellungnahme Deutscher Ju-

ristinnenbund). Um es mit den Worten vom Sprecher des Chaos Computer Club, Frank Rieger, zu formulieren, ist es unangemessen, besonders gefährdeten Frauen den Schutz der Anonymität zu entziehen und hier entgegenzuhalten, „*dass der Rechtsstaat sie schon schützen wird, wenn der besoffene Ex mit der Eisenstange vor der Tür*“ steht. Datenregister, welche zu erheblicher Gefährdung von ganzen Menschengruppen führen könnten, wie die historisch belasteten „Rosa Listen“ und Prostitutionsregister, sollten aus moralischen Gründen nicht eingerichtet werden.

Bewegungsdaten durch Smartphone-Nutzung

Neben den schon seit vielen Jahren vorgetragenen Argumenten gegen die Vorratsdatenspeicherung soll hier noch kurz auf einen technischen Aspekt hingewiesen werden. Wie unter anderem das mit dem Grimme Online Preis ausgezeichnete Blog netzpolitik.org aufzeigte, entstehen nach dem vorliegenden Entwurf zur Einführung der Vorratsdatenspeicherung durch die aktuell vorherrschende Form der Smartphone-Nutzung Bewegungsdaten einer völlig neuen Qualität. Aufgezeichnet werden genaue Bewegungsprofile aller Smartphone-Nutzern und dies sogar unabhängig davon, ob überhaupt telefoniert wird. Diese Daten sind ein Milliarden-Dollar Ziel. Ein derartiger Datenschatz würde eine Komplettanalyse der wirtschaftlichen und gesellschaftlichen Abläufe innerhalb Deutschlands ermöglichen.

Es steht zu befürchten, dass Cyberangreifern sich nicht in angemessener Weise um Richtervorbehalte oder den Schutz von Seelsorgern und Beratungsstellen kümmern würden. Ein paar einfache Datenbankabfragen liefern dann beispielsweise Politiker und Manager, die eine Alkoholberatungsstelle angerufen haben oder nach den Bewegungsdaten in einer Entzugsklinik behandelt wurden. Big Data als Alptraum.

Nicht nur wegen der zeitlichen Koinzidenz muss sich die Politik fragen lassen, wie für umfassende Überwachungsdaten eine reale Sicherheit versprochen werden kann, wenn sich zeitgleich selbst das wichtigste Verfassungsorgan reichlich hilflos gegenüber Cyberangriffen zeigt.

Wissenschaftliche Empfehlungen

Aus der Sicht theoriekundiger Praktiker_innen und praktisch orientierter Theoretiker_innen ergeben sich überraschend einfache Empfehlungen mit zu vernachlässigenden Kosten: **Starke Kryptographie mit extra Sicherheitsspielraum.**
Dies bedeutet auf der Algorithmenebene beispielsweise:

- Schlüssellänge größer gleich 4096 bit für RSA und DH
- die Verwendung von 256-bit Schlüssellänge für AES
- 512-bit Hash-Funktionen

Ohne volle Schlüsselkontrolle für die Anwendern und ohne lesbaren Code und offene Hardware helfen die besten kryptographischen Verfahren natürlich nicht gegen Geheimdiensthintertüren.

Open Source Sicherheit und Datensparsamkeit als Staatsaufgabe wahrnehmen

Open Source Software biete die Möglichkeit zum Auffinden von Hintertüren und Programmierfehlern. Eine Grundsicherheit für systemrelevante Open Source Programme sollte als Staatsaufgabe wahrgenommen werden. Daten, welche zur erheblichen Gefährdung von ganzen Menschengruppen führen könnten, sollten aus moralischen Gründen gar nicht erst erhoben werden.

Kryptographie und Offene Software sind mächtige Werkzeuge zur Sicherung der Digitalen Souveränität. Die Aufgabe die digitale Gesellschaft menschenwürdig zu gestalten, bleibt allerdings auch Aufgabe unseres freiheitlich demokratisch verfassten Gemeinwesens. Meinungsfreiheit, Datenschutz und Subsidiarität sind unsere gewachsenen Grundwerte, welche bescheiden und selbstbewusst in der weltweiten Diskussion eingebracht werden sollten.

RÜDIGER WEIS ist Diplom-Mathematiker und Kryptograph. Er lebt und arbeitet in Berlin-Wedding und ist Professor für Informatik an der Beuth-Hochschule für Technik Berlin.

Anmerkungen

1 Pressemitteilung vom 21.08.2013, Bonn, abrufbar unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Windows_TPM_Pl_21082013.html.