Gibt es einen sinnvollen Kompromiss zwischen der Verhinderung von Cybercrime und Datenschutz?

Marit Köhntopp und Andreas Pfitzmann
9. Juni 2001

Thema

Ein sinnvoller Kompromiss zwischen der Verhinderung von Cybercrime und Datenschutz wird dringend gesucht. Doch es ist unklar, ob ein solcher Kompromiss überhaupt existiert, der kompatibel ist zu der Informations- und Kommunikationstechnik (IT), die heute verfügbar ist oder die wir in den nächsten Jahrzehnten erwarten können. Dieser Artikel stellt die bekannten verfügbaren Datensicherheitstechniken vor und diskutiert deren möglichen Einsatz durch verschiedene Akteure. Außerdem betrachten wir die Seiteneffekte von Techniken zur Verhinderung und Aufklärung von Cybercrime: Führt man beispielsweise Hintertüren für die „Good Guys" als Technik zur Aufklärung von Cybercrime ein, werden diese auch von den „Bad Guys" genutzt werden, d.h. gleichzeitig ermöglichen diese Techniken Cybercrime. So zeigen die verfügbaren Techniken und ihre Seiteneffekte fundamentale Grenzen hinsichtlich des Erreichbaren.

Relevanz

Datenschutz oder genauer das, was im Englischen mit Privacy beschrieben wird, ist sowohl für jeden einzelnen Menschen wie auch für unsere demokratische Gesellschaft als Ganzes wichtig: Fühlen sich Menschen beobachtet, so wagen sie nicht, sich frei zu verwirklichen und sich gemäß ihren eigenen Interessen zu verhalten. Nicht nur Datenschutz, sondern auch Datensicherheit ist den Menschen ein Grundbedürfnis. In einer Welt, in der Cybercrime zunehmend eine Rolle spielt und schweren Schaden verursachen kann, ist es wichtig, Cybercrime so weit wie möglich zu verhindern, ohne dass zugleich Datenschutz und Datensicherheit gefährdet werden. Nur so können die Menschen Vertrauen zu einem Leben in der Informationsgesellschaft entwickeln.

1 Einführung

Das Wachstum der digitalen Kommunikation ging einher mit dem Erfolg des Internet als globalem Netz. Fast alle Kommunikation ist gesetzeskonform. Doch können Computernetze und elektronische Informationen auch zum Begehen von Straftaten genutzt werden. Dabei lassen sich verschiedene Typen von Cybercrime unterscheiden:

1. herkömmliche Kriminalität, bei der das Kommunikationsnetz genutzt wird, und
2. neue Formen spezifischer Computernetzkriminalität.

Im vorliegenden Artikel konzentrieren wir unseren Blick auf die Verhinderung von Cybercrime und nicht auf die Strafverfolgung. Dessen ungeachtet können Methoden der Strafverfolgung auch eine vorbeugende Wirkung haben.

Nach der Darstellung grundlegender Fakten zur IT-Sicherheit werden wir die Frage diskutieren, ob es einen sinnvollen Kompromiss zwischen Verhinderung und Aufklärung von Cybercrime einerseits und Datenschutz andererseits gibt.

2 Annahmen

Wenn wir einen sinnvollen Kompromiss suchen, müssen wir uns darüber klar werden, ob dieser abzielt auf
- Wünsche,
- Absichten,
- rechtliche Regelungen,
- durchsetzbare Regelungen,
- die Entwicklung, die Einrichtung, den Betrieb oder die Nutzung von IT, oder
- die Wirkungen des Netzes auf Einzelpersonen, Wirtschaft und Gesellschaft.

Auf der Suche nach solch einem Kompromiss müssen wir die Grundannahmen, von denen wir ausgehen, offenlegen: Wir müssen davon ausgehen, dass nur teilweise eine Kooperation der Staaten und der Industrie stattfindet; zugleich müssen wir mit effektiv offenen Grenzen für Informations- und Kommunikationstechnik (IT), Know-how und Bits umgehen (weltweiten Handel und globale Kommunikation voraussetzend).

Unter diesen Annahmen müssen wir die (Netz-)Wirkungen auf Einzelpersonen, Wirtschaft und Gesellschaft berücksichtigen, die bei jedem Vorschlag von rechtlichen Regulierungen und erwartetem Einfluss auf IT-Entwicklung, –Einrichtung, –Betrieb und –Nutzung vorherzusehen sind. Einen sinnvollen Kompromiss für die Lösung dieses Problems suchend, werfen wir zunächst einen Blick auf heutige IT-Datensicherheitstechniken und auf vorgeschlagene Methoden zur Verhinderung und Aufklärung von Cybercrime.

3 Verfügbare und bekannte Datensicherheitstechniken

Zum Zweck der Verhinderung von Cybercrime sollten die Nutzer ihre Rechnersysteme und ihre Daten (einschließlich der Transaktionsdaten und Kommunikationsspuren, sofern vorhanden) vor Angriffen schützen. Bei der Erörterung von Datensicherheitstechniken berücksichtigen wir sämtliche beteiligten Parteien.

Mehrseitige Sicherheit bedeutet Sicherheit für alle Beteiligten, wobei jede(r) anderen nur minimal zu vertrauen braucht:
- Jede(r) hat individuelle Schutzziele.
- Jede(r) kann seine Schutzziele formulieren.
- Konflikte werden erkannt und Kompromisse werden ausgehandelt.
- Jede(r) kann seine/ihre Schutzziele im Rahmen des ausgehandelten Kompromisses durchsetzen.

Ähnlich wie die Aufklärung die Menschen von der Unterdrückung durch abergläubisches Denken und autoritäre politische Modelle befreit hat, hat die Technik für mehrseitige Sicherheit das Potenzial, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un-)Sicherheit zu befreien.

Einige dieser Techniken können von verschiedenen Beteiligten unilateral genutzt werden. Bei anderen ist eine bilaterale Kooperation notwendig, z.B. die Zusammenarbeit der beiden Kommunikationspartner. Wieder bei anderen ist eine trilaterale Kooperation nötig. Ein Beispiel sind rechtlich bindende digitale Signaturen, die nicht nur der Kooperation von zumindest zwei Kommunizierenden bedürfen, sondern weiterhin mindestens einer vertrauenswürdigen dritten Partei, die die öffentlichen Schlüssel zertifiziert. Bei anderen Techniken ist sogar die multilaterale Zusammenarbeit einer großen Zahl von unabhängigen Parteien notwendig. Wir verwenden diese Unterscheidung, um einen kurzen strukturierten Überblick über die bekannten Techniken für mehrseitige Sicherheit zu geben (siehe auch [Pfit_00]).

3.1 Unilateral nutzbare Techniken

Unilaterale Techniken können durch jede der Parteien selbst bestimmt werden. Es bedarf hierfür weder einer Koordination noch eines Aushandelns hinsichtlich ihrer Verwendung. Wichtige unilaterale Techniken für mehrseitige Sicherheit sind:

- *Werkzeuge, die selbst unerfahrenen Benutzern helfen*, ihre Schutzziele zu formulieren, im Bedarfsfall für jede einzelne Anwendung oder jede einzelne Aktion [PSWW_98, WoPf_00].
- *(Portable) Geräte, die für ihre Benutzer sicher sind,* als Basis jeder Datensicherheit. Die Geräte benötigen wenigstens ein Mindestmaß an physischem Schutz, der die direkte Ein- und Ausgabe für ihre Benutzer umfasst [PPSW_99], und im Fall von multifunktionalem Einsatz ein Betriebssystem mit feingestufter Zugriffskontrolle und mit einer Rechteverwaltung für verschiedene Anwendungen nach dem Prinzip der geringstmöglichen Privilegierung.
- *Verschlüsselung* von lokalen Speichermedien, um die Inhalte vertraulich zu halten und/oder zu authentisieren.
- *Verstecken* von geheimen Daten in lokalen multimedialen Inhalten oder in lokalen Dateisystemen [AnNS_98] unter Verwendung von Steganographie, mit dem Ziel, nicht nur den Inhalt der geheimen Daten zu schützen, sondern auch ihre Existenz geheimzuhalten.
- *Watermarking* oder *Fingerprinting* digitaler Daten unter Nutzung steganographischer Techniken, um die Autorschaft oder Urheberrechtsverletzungen besser nachweisen zu können.
- Ausschließliche Nutzung von *Software, deren Quellcode veröffentlicht und von vielen untersucht ist* oder *deren Sicherheit von vertrauenswürdigen unabhängigen Instanzen zertifiziert* ist, die Zugriff auf den vollständigen Quellcode und alle Werkzeuge zur Generierung des Objektcodes hatten. Am besten ist eine Kombination beider Ansätze hinsichtlich möglichst vieler der verwendeten Software-Bestandteile. Es bedarf zumindest des Einsatzes einer der beiden Ansätze, um einigermaßen sicher sein zu können, dass die verwendete Software keine trojanischen Pferde enthält. Das Gleiche gilt mehr oder weniger für *Hardware*, bei der alle Quellen und Werkzeuge, die bei der Gestaltung und der Produktion eingesetzt worden sind, auf das Nichtvorhandensein von trojanischen Pferden hin überprüft werden müssen.

3.2 Bilateral nutzbare Techniken

Bilaterale Techniken können nur genutzt werden, wenn die Kommunikationspartner zusammenarbeiten. Dies setzt für ihren Gebrauch eine gewisse Koordination und Absprache voraus. Wichtige bilaterale Techniken für mehrseitige Sicherheit sind:

- *Werkzeuge*, um Schutzziele und Sicherheitsmechanismen bilateral *auszuhandeln* [PSWW_98].
- *Kryptographische und steganographische Mechanismen*, um Kommunikationsinhalte zu schützen, siehe Abb. 1 und 2.

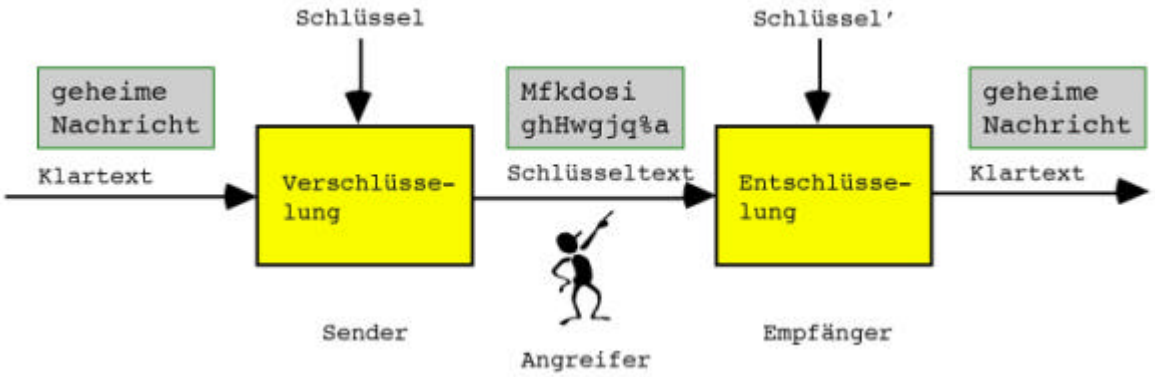

Abb. 1: Kryptographische Mechanismen, um Vertraulichkeit und Integrität der Kommunikationsinhalte zu schützen

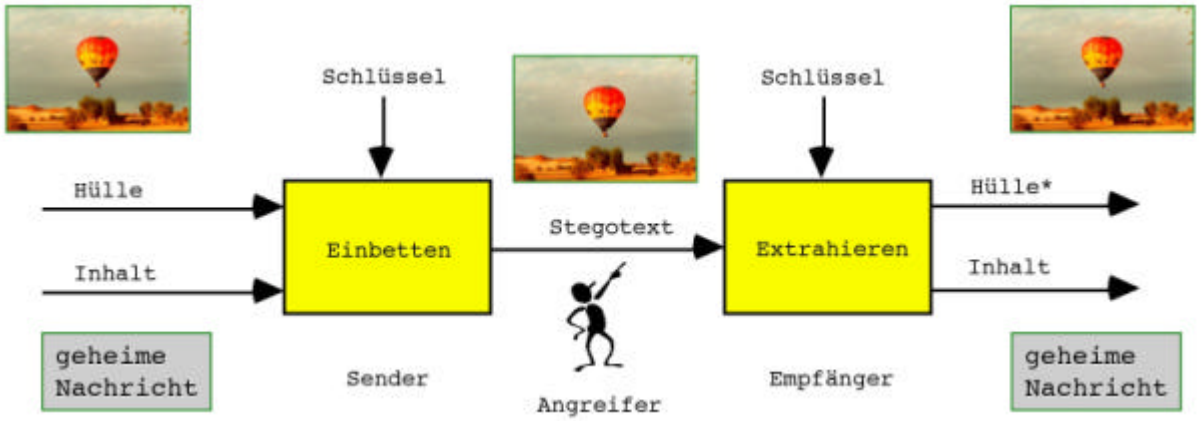

Abb. 2: Steganographische Mechanismen zum Verbergen der Existenz vertraulicher Kommunikationsinhalte

3.3 Trilateral nutzbare Techniken

Trilaterale Techniken setzen für ihre Nutzung eine dritte Partei voraus, die besondere Aufgaben für die anderen beteiligten Parteien erfüllt. Dies bedeutet, dass mehr Koordination und Aushandlung bei deren Nutzung notwendig ist im Vergleich zu den unilateralen und in der Regel auch den bilateralen Techniken. Wichtige trilaterale Techniken für mehrseitige Sicherheit sind:

- *Werkzeuge*, um Sicherheitsmechanismen trilateral *auszuhandeln*, z.B. für Zurechenbarkeit.
- Eine *Public-Key-Infrastruktur* (PKI), die Nutzern zertifizierte öffentliche Schlüssel anderer Nutzer zur Verfügung stellt, um deren digitale Signatur zu überprüfen und um den Nutzern die Möglichkeit zu geben, ihren eigenen öffentlichen Schlüssel zurückzuziehen, wenn der entsprechende private Schlüssel kompromittiert worden ist.
- *Sicherheitsgateways*, um Inkompatibilitäten bzgl. Sicherheitsmechanismen oder Teilen von diesen zu überbrücken. Sicherheitsgateways funktionieren gut in Bezug auf Mechanismen für Integrität und Zurechenbarkeit; sie sind aber nur von fragwürdigem Wert hinsichtlich

Vertraulichkeit und Anonymität. Natürlich können Sicherheitsgateways keine Unvereinbarkeiten bzgl. Schutzzielen auflösen.

- Mechanismen zur Schaffung von *digitalen Pseudonymen* als geeignete Kombination von Anonymität und Zurechenbarkeit [Chau_81]. Insbesondere gibt es Mechanismen, um sicher Signaturen (die für bestimmte Befugnisse stehen, sog. Beglaubigungen (Credentials)) zwischen verschiedenen Pseudonymen derselben Partei zu transferieren [Chau_85, Chau_90, Chau_92]. Dies wird *„Transfer von Signaturen zwischen Pseudonymen“* genannt.
  Beim Einsatz von Pseudonymen für einen zurechenbaren Werteaustausch gibt es verschiedene Möglichkeiten hinsichtlich der Aufgaben der einbezogenen dritten Partei:
  - Identifikation des Nutzers im Betrugsfall (Pseudonyme sind zertifiziert und die Zertifizierungsstelle kennt die wirkliche Identität), d.h. der Pseudonymträger kann nicht überprüfen, ob sein Pseudonym aufgedeckt wurde und damit seine Anonymität nicht mehr gewährleistet ist.
  - Geldhinterlegung bei einem aktiven Treuhänder zur Verhinderung von Betrug, wobei die Pseudonyme für die anderen Beteiligten völlig anonym bleiben, d.h. die Anonymität wird durch die Pseudonymträger selbst gesteuert.

3.4 Multilateral nutzbare Techniken

Multilaterale Techniken können nur zum Einsatz kommen, wenn eine größere Zahl unabhängiger Parteien zusammenwirken. Dies setzt in einem großen Maß Koordination und ggf. auch Aushandlung voraus. Wichtige multilaterale Techniken für mehrseitige Sicherheit sind:

- *Werkzeuge*, um multilateral Schutzziele und Sicherheitsmechanismen *auszuhandeln*, z.B. für Anonymität und Unbeobachtbarkeit.
- Mechanismen, um *Anonymität, Unbeobachtbarkeit und Unverkettbarkeit* zu erreichen bei
  - Kommunikation, d.h. zu schützen, wer wann von wo mit wem wohin kommuniziert [Chau_81, Chau_85, PfWa_87, CoBi_95, FeJP_96, JMPP_98, ReRu_99, GoRS_99], siehe Abb. 3,
  - Zahlungen, d.h. zu schützen, wer wann an wen welchen Betrag für welche Leistung bezahlt [Chau_89, AJSW_97], und
  - Werteaustausch, d.h. elektronisches Einkaufen vor Beobachtung zu schützen [BüPf_90, AsSW_97],

  ohne Integrität, Verfügbarkeit oder Zurechenbarkeit zu kompromittieren.

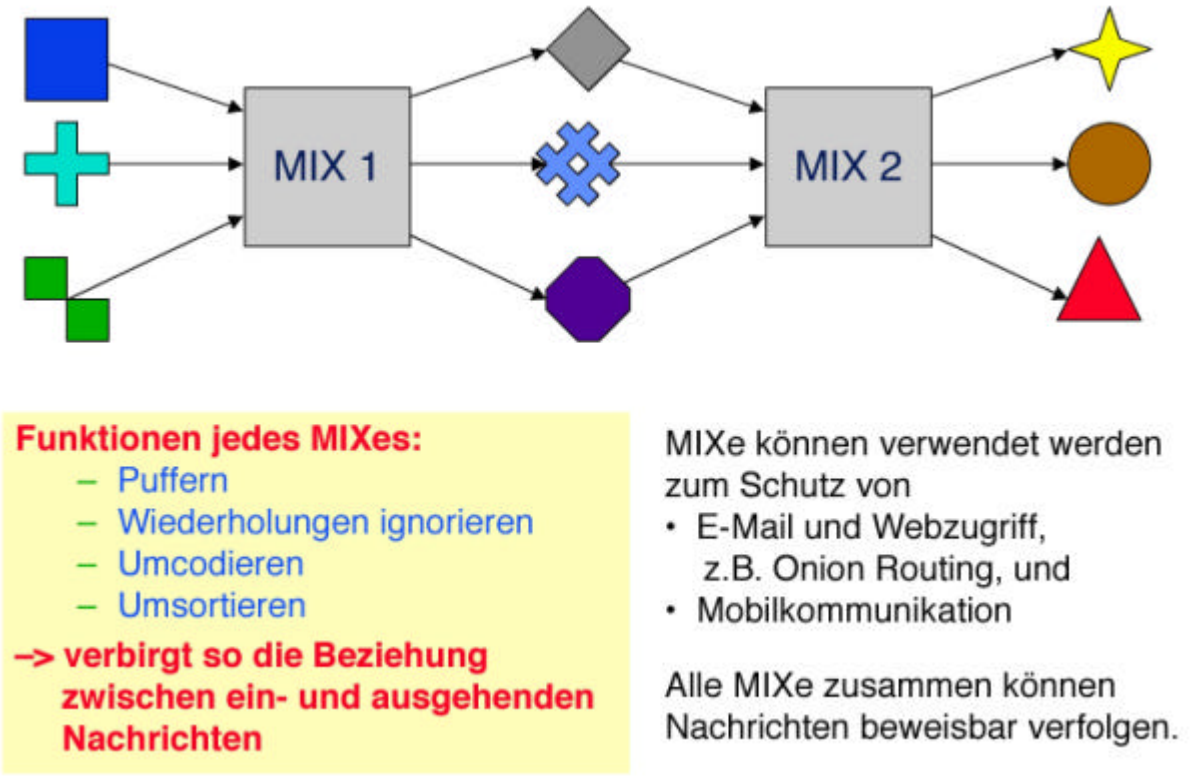

Abb. 3: Anonymität, Unbeobachtbarkeit und Unverkettbarkeit bei Kommunikation

4 Bewertung von Reifegrad und Wirksamkeit der Datensicherheitstechniken

Tabelle 1 stellt unsere Bewertung von Reifegrad und Wirksamkeit der in den vorigen Abschnitten beschriebenen Datensicherheitstechniken dar. Die Tabelle sollte von oben nach unten gelesen werden: Eine Datensicherheitstechnik in einer bestimmten Zeile ist Voraussetzung, bevor eine darunter aufgeführte Technik wirksam sein kann. In einigen Fällen werden Beispiele hinter dem Semikolon aufgeführt.

	Stand der öffentlichen Forschung	Demonstratoren und Prototypen	Verfügbare Produkte	Weit verbreitete Produkte
Physischer Schutz	kaum seriöse Publikationen	schwer zu beurteilen	schwer zu beurteilen; Me-Chip	sehr schlecht; Chipkarten
Sicherheitsevaluierung von IT	akzeptabel	schwer zu beurteilen	schwer zu beurteilen	schwer zu beurteilen
Sicherheit in Betriebssystemen	sehr gut	gut	schlecht; Windows NT, Windows 2000, Linux, Mac OS X	sehr schlecht; Windows 98, Windows ME, Windows CE, Mac OS 9
Kryptographie	sehr gut	gut	gut; PGP 2.6.x	akzeptabel; PGP 5.x, PGP 6.x
Steganographie	gut	akzeptabel	sehr schlecht	sehr schlecht
PKI	sehr gut	gut	schwer zu beurteilen	–
Sicherheitsgateways	gut	akzeptabel	–	–
Mechanismen für Anonymität, Unbeobachtbarkeit und Unverkettbarkeit	sehr gut	gut	akzeptabel; Onion Routing, Freedom	schlecht; Proxies
Digitale Pseudonyme	sehr gut	gut	gut; PGP 2.6.x	akzeptabel; PGP 5.x, PGP 6.x
Transfer von Signaturen zwischen Pseudonymen	gut	–	–	–
Werkzeuge, die beim Formulieren und Verhandeln helfen	gut	akzeptabel	–	–
Integration dieser Techniken	akzeptabel	schlecht	schlecht	sehr schlecht

Tabelle 1: Reifegrad und Wirksamkeit von Datensicherheitstechniken

Man kann sehen, dass das schwächste Glied in der Sicherheitskette heute beim Endgerät der Nutzer liegt, insbesondere bei dessen physischem Schutz und dessen Betriebssystem. Um beides zu verbessern, muss noch viel getan werden.

Offensichtlich sind die Evaluierung von IT und die Integration von Datensicherheitstechniken diejenigen Herausforderungen für die Wissenschaft, die den größten Einfluss auf IT-Sicherheit haben.

5 Ansätze zur Verhinderung von Cybercrime und deren Nebenwirkungen

Viele der diskutierten Ansätze zur Verhinderung oder Aufklärung von Cybercrime zielen darauf ab, IT-Sicherheit zu reduzieren, um Strafverfolgern einen Zugang zu ermöglichen. Die meisten Mechanismen basieren auf dem Einbau von Hintertüren [STOA_00], beispielsweise durch Einschleusen von trojanischen Pferden in Betriebssysteme oder durch Key Escrow und Key Recovery bei Verschlüsselungssystemen. Wie z.B. in [AAB+_98] beschrieben, können solche Hintertüren nicht nur von befugten Strafverfolgern verwendet werden, sondern auch von Kriminellen.

Hinzu kommt, dass kein Staat einer aus einem anderen Staat importierten Informationstechnik trauen kann, da Hintertüren eingebaut sein könnten.

Die Grundrechte auf Datenschutz und Anonymität, die in unserer Offline-Welt der Standard sind, kollidieren mit den diskutierten Pflichten für die Internet-Nutzer, authentische Spuren zu hinterlassen. Die Forderung gegenüber den Internet-Providern, sämtlichen Datenverkehr zu protokollieren und aufzubewahren, bringt zudem nicht nur Risiken für den Datenschutz durch möglichen Missbrauch, sie ist absolut unverhältnismäßig: Jeder kann diese Protokollierung ins Leere laufen lassen, indem er kryptographische oder starke steganographische Werkzeuge nutzt und/oder Anonymitätsmechanismen, die in Ländern gehostet werden, die außerhalb der Reichweite des heimischen Rechts liegen, jedoch gut ans Internet angebunden sind und damit gut erreichbar sowohl für datenschutzbewusste Bürgerinnen und Bürger wie für Kriminelle. Die wirkliche Bedrohung für die Verhinderung und Aufklärung von Cybercrime besteht darin, dass solche unverhältnismäßigen Mittel dazu tendieren, eine Solidarisierung zwischen datenschutzbewussten Menschen und möglichen Kriminellen zu schaffen. Alle Erfahrungen bei der Bekämpfung organisierter Kriminalität zeigen, dass eine solche Solidarisierung das größte Hindernis für einen Erfolg ist. Phil Zimmermann hat dies recht präzise auf den Punkt gebracht: „Wenn Datenschutz kriminalisiert wird, werden nur noch Kriminelle Datenschutz haben“ („If privacy is outlawed, only outlaws will have privacy“).[1] Wir meinen, die Cyber-Polizei wäre schlecht beraten, wenn sie diesen Weg beschritte.

Wie aus Tabelle 1 zu sehen ist, ist der Stand öffentlicher Forschung im Hinblick auf Datensicherheitstechniken in den meisten Bereichen recht gut. Es bedarf der Anstrengung, dies in Standardprodukte einzubauen, um allen Nutzern in offenen Netzes den Gebrauch zu ermöglichen. Weniger Aufwand ist nötig, um die Kommunikation innerhalb geschlossener Gruppen kompetenter Nutzer zu schützen. Dies bedeutet, dass kriminelle Organisationen genauso ihre eigenen Datensicherheitswerkzeuge schaffen und nutzen können wie jede andere geschlossene Nutzergruppe. So können Einschränkungen, z.B. Krypto-Regulierungen, leicht umgangen werden [FJMP_96].

Von diesem Blickwinkel aus erscheint es logisch, aktive Angriffe durch Strafverfolger zu diskutieren, z.B. Denial-of-Service-Angriffe (DoS), das Freisetzen von Viren oder Inhaltsveränderungen auf Speichermedien von verdächtigen Subjekten[2] [Wals_96]. Derartige Informationskriegstechniken mögen nach dem Motto „Der Zweck heiligt die Mittel“ effektiv funktionieren. Doch sind solche „Lizenzen zum Hacken“ nicht nur aus rechtlicher Sicht fragwürdig, auch die Echtheit der ermittelten Beweismittel wird mit solchen manipulativen Angriffen massiv in Frage gestellt.

Daher müssen wir uns bewusst sein, dass die diskutierten Methoden zur Bekämpfung von Cybercrime nicht nur eine starke Spannung zu Datenschutz haben, sondern auch zu IT-Sicherheit:
- Viele Werkzeuge, die für Datensicherheitstests benötigt werden, können auch zum Hacken unsicherer Systeme genutzt werden.
- Hintertüren können nicht nur zur Überwachung durch befugte Stellen genutzt werden, sondern auch zum Manipulieren von Spuren. Außerdem kann beides genauso durch Befugte wie durch Unbefugte erfolgen.

---

[1] Phil Zimmermann, Why do you need PGP? 5. Juni 1991, http://www.pgpi.org/doc/whypgp/en/.

[2] Beispielsweise mit Hilfe der Software „D.I.R.T. – Data Interception by Remote Transmission“ der US-Firma Codex Data Systems (http://www.codexdatasystems.com/menu.html). Weitere Informationen zu D.I.R.T. bei Cryptome, http://cryptome.org/dirty-secrets2.htm, sowie im Artikel „No more secrets“ von Florian Rötzer, Heise Telepolis, 6. Juni 2001, http://www.heise.de/tp/deutsch/inhalt/te/7830/1.html.

Andererseits liefern gerade Datensicherheitstechniken selbst die Werkzeuge zur Verhinderung derjenigen Formen von Cybercrime, die spezifisch für Computernetze sind: Öffentliche Forschung und Entwicklung in diesem Bereich wird zu sichereren Systemen führen, in denen sich die Nutzer selbst schützen können.

6 Schlussfolgerungen

Eine Interpretation dieser Ergebnisse führt uns zu folgenden Feststellungen:

1. IT-Sicherheit ist erschreckend unterentwickelt, und der Versuch, sie effektiv zu verbessern, ist ein ehrgeiziges Unterfangen.
2. Sämtliche Hintertüren, insbesondere diejenigen, die für die „Good Guys" eingerichtet wurden, werden auch von den „Bad Guys" benutzt werden, d.h. diese Techniken zur Verfolgung von Cybercrime sind unzweifelhaft zugleich Techniken, die Cybercrime ermöglichen.
3. Egal was auch unternommen wird, clevere „Bad Guys" haben wirksame Techniken zur Geheimhaltung,
   - was sie speichern und was und mit wem sie von wo wohin kommunizieren oder gar
   - ob sie überhaupt speichern und kommunizieren.

Wird daher Datenschutz in Bezug auf IT juristisch eingeschränkt, so werden nur Kriminelle uneingeschränkten Datenschutz haben.

Insbesondere ist es von großer Wichtigkeit, dass die Bekämpfung von Cybercrime nicht die Entwicklung der IT-Sicherheit verlangsamen oder sogar weiter schwächen darf[3]. In der aktuellen Situation sollten Strafverfolger nur unter streng kontrollierten Bedingungen das Recht und die Möglichkeit haben, heute vorhandene Schwächen der IT bei Datensicherheit auszunutzen. Keineswegs sollten sie das Recht behalten oder gar bekommen, den Einbau weiterer Schwächen durchzusetzen.

Langfristig sollten Mängel bei der Datensicherheit in der Informations- und Kommunikationstechnik verschwinden. Alle Nutzer sollten befähigt werden, über ihre Datensicherheit und ihren Datenschutz selbst zu bestimmen. Strafverfolger sollten Techniken nutzen, mit denen wirksam einzelne Personen oder kleine Gruppen überwacht werden können, die aber nicht so ausgelegt sind, dass sie eine Massenüberwachung derjenigen erlauben, die sich nicht selbst schützen. Derartige Techniken für Individualüberwachung sind außerhalb der IT-Infrastrukturen richtig und wirksam angesiedelt. Selbstverständlich würde dadurch der Arbeitsplatz von manchem Internet-Ermittler unbequemer. Es geht aber nicht um deren Bequemlichkeit, sondern um wirksame und effiziente Maßnahmen gegen Cybercrime ohne dramatische Nebenwirkungen. Wir müssen im Auge behalten, dass Demokratie nicht dadurch verteidigt werden kann, dass eine IT-Infrastruktur à la Orwell aufgebaut wird.

In jedem Fall brauchen wir eine offene Diskussion über Verhinderung und Aufklärung von Cybercrime, an der sich Strafverfolgungsbehörden, Datenschutzorganisationen, IT-Industrie, Nutzer

---

[3] Ähnlich auch [EU_01]: „Die berechtigten Bedenken in bezug auf Computerkriminalität erfordern effiziente polizeiliche Ermittlungen. Diese rechtlichen Bedenken sollten jedoch keine Lösungen schaffen, bei denen rechtliche Erfordernisse zu einer Schwächung der Sicherheit von Kommunikations- und Informationssystemen führen."

und Politiker beteiligen. Aus dieser Perspektive betrachten wir das übereilte Vorgehen bzgl. der Cybercrime-Convention im Europarat als eine vertane Chance.

Auf der Suche nach einem sinnvollen Kompromiss kommen wir zu dem Schluss, dass dieser nicht durch eine Schwächung von IT-Sicherheit erlangt werden kann. Werkzeuge für Datenschutz und Datensicherheit müssen vielmehr verbessert werden, um Nutzern einen besseren Schutz zu bieten, d.h. um dadurch Cybercrime zu verhindern. Auf keinen Fall kann Technik allein die verschiedenen Erscheinungsformen von Kriminalität verhindern. Wir brauchen „policy action instead of police actionism“[4] („aktive Politik, nicht polizeilichen Aktionismus“). Wir müssen uns bewusst sein, dass es nicht nur darum geht, mit potenziellen finanziellen Verlusten, gegen die wir vielleicht sogar versichert sind, fertig zu werden. Statt dessen müssen wir unsere demokratische Gesellschaft in ihrer Gesamtheit gegen Schäden verteidigen. Dabei dürfen Datenschutz und Datensicherheit nicht aufs Spiel gesetzt werden.

Literatur

[AAB+_98] Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier: The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, Final Report: 27. Mai 1997, aktualisiert: 8. Juni 1998; http://www.cdt.org/crypto/risks98/.

[AJSW_97] N. Asokan, Phillipe A. Janson, Michael Steiner, Michael Waidner: The State of the Art in Electronic Payment Systems; Computer 30/9 (1997) 28-35.

[AnNS_98] Ross Anderson, Roger Needham, Adi Shamir: The Steganographic File System; Information Hiding, 2nd Workshop, Portland, Oregon, LNCS 1525, Springer, Berlin 1998, 73-82.

[AsSW_97] N. Asokan, Matthias Schunter, Michael Waidner: Optimistic Protocols for Fair Exchange; 4th ACM Conference on Computer and Communications Security, Zürich, April 1997, 6-17.

[BüPf_90] Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

[Chau_81] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

[Chau_85] David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

[Chau_89] David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proc. of the IFIP WG 11.6 Intern. Conference; Laxenburg (Austria), 1987, North-Holland, Amsterdam 1989, 69-93.

[Chau_90] David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt ‘90, LNCS 453, Springer, Berlin 1990, 246-264.

[Chau_92] David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

[CoBi_95] David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

[EU_01] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Sicherheit der Netze und Informationen –

[4] Dieter Klumpp, Geschäftsführer der Alcatel SEL Stiftung für Kommunikationsforschung, Stuttgart 2001, ähnlich in seiner Rede „Electronic Government und Bürgernetze – Electronic Government und Bürgernetze – Zukunftsstrategien für öffentliche und private Verwaltungen“, Deutscher Städtetag, 26. April 2001 Stuttgart.

Vorschlag für einen europäischen Politikansatz; 6. Juni 2001; http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_de.pdf.
[FeJP_96] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy; Information Hiding, 1st Workshop, Cambridge, UK, LNCS 1174, Springer, Berlin 1996, 121-135.
[FJMP_96] Elke Franz, Anja Jerichow, Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best; Information Hiding, LNCS 1174, Springer, Berlin 1996, 7-21.
[GoRS_99] David Goldschlag, Michael Reed, Paul Syverson: Onion Routing for Anonymous and Private Internet Connections; Communications of the ACM 42/2 (1999) 39-41.
[JMPP_98] Anja Jerichow, Jan Müller, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol; IEEE Journal on Selected Areas in Communications 16/4 (Mai 1998) 495-509.
[Pfit_00] Andreas Pfitzmann: Multilateral Security: Enabling Technologies and Their Evaluation, in: R. Wilhelm (Hg.): Informatics – 10 Years Back, 10 Years Ahead, LNCS 2000, Springer, Berlin 2001, 50-62.
[PfWa_87] Andreas Pfitzmann, Michael Waidner: Networks without user observability; Computers & Security 6/2 (1987) 158-166.
[PPSW_99] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trustworthy User Devices; in: G. Müller, K. Rannenberg (Hg.): Multilateral Security in Communications, Addison-Wesley, München 1999, 137-156.
[PSWW_98] Andreas Pfitzmann, Alexander Schill, Andreas Westfeld, Guntram Wicke, Gritta Wolf, Jan Zöllner: A Java-based distributed platform for multilateral security; IFIP/GI Working Conference „Trends in Electronic Commerce“, Hamburg, LNCS 1402, Springer, Berlin 1998, 52-64.
[ReRu_99] Michael K. Reiter, Aviel D. Rubin: Anonymous Web Transactions with Crowds; Communications of the ACM 42/2 (1999) 32-38.
[STOA_00] STOA – Scientific and Technological Options Assessment, European Parliament: Development of surveillance technology and risk of abuse of economic information, 1998-2000; http://www.europarl.eu.int/stoa/publi/pop-up_en.htm.
[Wals_96] Gerard Walsh: Review of Policy relating to Encryption Technologies (Walsh-Report), 1996 erstellt vom Australian Attorney-General’s Department, verschiedene Teile 1997-1999 veröffentlicht; http://www.efa.org.au/Issues/Crypto/Walsh/ (Website von Electronic Frontiers Australia).
[WoPf_00] Gritta Wolf, Andreas Pfitzmann: Properties of protection goals and their integration into a user interface; Computer Networks 32 (2000) 685-699.