Die Reaktion der Gesellschaft für Informatik auf die Snowden-Enthüllungen: Un/Sicherheit-FAQ und E-mail-Verschlüsselung

Klaus-Peter Löhr, Berlin

GI-SECMGT Workshop, 9.5.2014

Scott McNealy (Sun Microsystems, 1999):

„You have zero privacy anyway. Get over it “

Edward Snowden (Booz Allen Hamilton, July 2013):

„They are getting everyone's calls, everyone‘s call records and everyone's internet traffic as well.“

Dilma Rousseff (Brazilian president, September 2013):

„Without the right to privacy, there is no real freedom of speech or freedom of opinion, and therefore, there is no actual democracy“.

Snowden und die GI: Rückblick

6.-9. Juni: Erste Berichte im „Guardian“ und Interview mit Snowden

11. Juni: Pressemitteilung des PAK zu De-Mail: *„Schriftverkehr mit Behörden muss standardmäßig Ende-zu-Ende verschlüsselt werden“*

26. Juni: Pressemitteilung des PAK *„Geheimdienste kontrollieren die weltweite Internetkommunikation“*

1. Juli: Erste Titelgeschichte des „SPIEGEL“ zur NSA-Affäre

23. Juli: Simone Rehm (GI-Vizepräsidentin) regt an, eine *„FAQ-Liste zu Sicherheit und Unsicherheit im Internet“* zu veröffentlichen, um damit zur Aufklärung beizutragen

22. August: Rudolf Bayer (TU München) auf der GI-Website:
„E-Mail-Verschlüsselung: ein Selbstversuch und eine Anleitung“

2. September: Pressemitteilung *„GI zur Spähaffäre: Informatiker klären auf“*
mit „FAQ-Liste zur Überwachungsaffäre 2013“
(„Sicherheit und Unsicherheit im Internet“)

23. September: Pressemitteilung des PAK: *„NSA: Back Doors in 80.000 strategischen Servern weltweit“*

23. September: Pressemitteilung der FG Angewandte Kryptographie:
„Kryptographie schützt Grundrechte“

2. Oktober: Pressemitteilung *„GI empfiehlt Verschlüsselung“*
(mit Verweis auf FAQ-Liste und Ankündigung konkreter Aktionen)

Die FAQ-Liste zur Überwachungsaffäre

Unmittelbare Resonanz

10000 – 15000 Zugriffe pro Tag
direkt nach Erscheinen, dann schnell abflauend.
3.9., 8:30: „GI-Server überlastet!“

130 – 140 Kommentare insgesamt,
mittlere bis gute Qualität,
punktuell harsche technische Kritik von Experten

Bericht bei Heise, verhaltene Kritik „zu unpolitisch“.
67 Kommentare (viel Blabla und Hickhack):
„Gute Fragen, schwache Antworten, merkelhaft“
„Keine Hilfen, wie man sich schützen kann“

(sonst praktisch nichts im Netz zu „Informatiker klären auf“)

Struktur der FAQ-Liste

- allgemeine und politische Fragen
- technische und ökonomische Fragen
- Ausspähung und mögliche Abwehr
- juristische Fragen

Jeweils interaktiv kommentierbar (mit Thread-Struktur)

Allgemeine und politische Fragen

A7 Dürfen Polizei und Geheimdienste die neueste Technik nutzen, um Verbrechen aufzudecken oder zu verhindern? Müssen Polizei und Geheimdienste über gute Internet-Kompetenz und moderne Analyse-Möglichkeiten verfügen?

„... sie dürfen (mit gesetzlicher Grundlage) ...
... ‚Waffengleichheit' ....."

6 Kommentare: aber keine flächendeckende Überwachung!

Aber: was ist ‚neueste Technik'?
E-mail, Data Mining, Bundestrojaner, Stuxnet, Heartbleed, ... ?
→ dürftige Fragestellung (und Antwort)

Die tiefergehenden Fragen:

- Dürfen die Behörden bekannte Sicherheitslücken nutzen?
- Dürfen die Behörden *unbekannte* Sicherheitslücken nutzen?
- *Müssen* die Behörden unbekannte Sicherheitslücken *bekannt machen* (um Bürger und Staat zu schützen, eventuell sogar vor Cyberterror) ?

  Pressemitteilung der GI vom 30.8.2007 (!):
  „ ... Die GI fordert ferner den Gesetzgeber auf, u.a. Behörden zur Veröffentlichung aller ihnen bekannten Sicherheitslücken zu verpflichten und die Verheimlichung von Sicherheitslücken zu sanktionieren. ...“

The White House, 28.4.2014:

„ ..... While we had no prior knowledge of the existence of Heartbleed, this case has re-ignited debate about whether the federal government should ever withhold knowledge of a computer vulnerability from the public. .....

..... We have also established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure. This interagency process helps ensure that all of the pros and cons are properly considered and weighed. .....“

Bruce Schneier, 10.3.2014: *(„Exploitation vs. Attack“)*

„ .....Much of the current debate in the U.S. is over what the NSA should be allowed to do, and whether limiting the NSA somehow empowers other governments. That's the wrong debate. We don't get to choose between a world where the NSA spies and one where the Chinese spy. Our choice is between a world where our information infrastructure is vulnerable to all attackers or secure for all users. .....“

A9 Was kann eine Fachgesellschaft wie die GI tun? Was hat die GI bisher unternommen?

„... FB Sicherheit ... PAK Datenschutz und IT-Sicherheit ...

... *sollte* sich für Ombudsmann einsetzen ...
... *kann* sich mit europäischen Schwestergesellschaften für politische Vereinbarungen einsetzen, die die Bürger vor Übergriffen fremder Geheimdienste schützen ...
... *wird* E-mail-Verschlüsselung (über den von Herrn Prof. Bayer gegebenen Anstoß hinaus) verstärkt propagieren ...“

6 Kommentare: alle fordern mehr Einsatz für Verschlüsselung
FAQ-Redaktion am 2.10.: „heutige Pressemeldung dazu!“

Technische und ökonomische Fragen

B1 Ist es technisch möglich, den Telefon- und E-Mailverkehr aufzuzeichnen? Nur die Verbindungsdaten oder auch die Inhalte?

„... ja (müssen aber wieder gelöscht werden) ...“
Gute Frage – aber *keine* Antwort zu E-Mail-Verkehr

10 Kommentare kritisieren mangelnde Vollständigkeit und Präzision der Antworten

B2 Was ist leichter abzuhören: eine WLAN-Verbindung oder eine Verbindung mittels Kabel, oder macht das keinen Unterschied?

„... Kabel ist etwas sicherer ...
... Verschlüsselung in jedem Fall erforderlich ...“

8 Kommentare, hauptsächlich zu Verschlüsselungsfragen,
mit Kritik an diesbezüglich technisch nachlässigen Antworten

B7 Existieren Hintertüren, undokumentierte Funktionen in Standardsoftware und Betriebssystemen sowie unveröffentlichte Sicherheitslücken?

„... alles ist möglich ...“

7 Kommentare mit pro/contra *quelloffene Software*
(Heartbleed kam erst später ;-)

bei Heise: „... Antwort verschleiert, dass es Unterschiede zwischen den Betriebssystemen geben könnte ...“

B8 Gibt es hundertprozentige Sicherheitsmaßnahmen gegen Penetration und Überwachung?

„... mit genügend Aufwand kann jedes System geknackt ...“

7 Kommentare: Diskussion von Krypto-Sicherheit sowie Kritik an pauschaler Fragestellung und Antwort

B10 Was bedeutet Wirtschaftsspionage?
Welche Folgen hat Wirtschaftsspionage?
Ist auch Sabotage möglich?

„... Beschaffung von Informationen durch konkurrierende Organisationen....“

(Falsch; das wird gewöhnlich als *Industriespionage* bezeichnet.
Wirtschaftsspionage ist das, was die NSA macht.
Ein Kommentator weist auch darauf hin.)

Ausspähung und mögliche Abwehr

C4 Mit welchen Sicherheitsmaßnahmen kann ich mich privat oder mein Unternehmen schützen – meine Kommunikation und meine gespeicherten Daten?

„Hundertprozentige Sicherheit gibt es nicht. ...
... Verschlüsselung ... Zugangskontrolle ...
... Daten sind auf Papier sicherer als im/am Netz“

(wenig hilfreich)

(wenig kommentiert)

C5 Wie verschlüssele ich?
Muss mein Kommunikationspartner auch verschlüsseln oder reicht es, wenn ich das tue?

„... symmetrische ... asymmetrische Verschlüsselung ...
... Tipps zu Verschlüsselungsprogrammen finden sich im Internet.“

16 Kommentare, darunter dieser:
„Tut mir leid, aber ‚Tipps zu Verschlüsselungsprogrammen finden sich im Internet‘ reicht nicht als Aussage der GI.“

Im übrigen klären sich die Diskutanten wechselseitig über Verschlüsselungstechnik auf ;-)

C7 Gibt es Unterschiede bei Suchmaschinen im Internet, was Datenspeicherung und Überwachung angeht?

„... ja ...“

16 Kommentare! Verschiedene Suchmaschinen-Kenner kritisieren diverse Schwächen und Fehler in der Antwort

Juristische Fragen

D1 Welche Rechte haben deutsche Behörden?

Erschöpfende Antwort *(2 Seiten!)*

5 Kommentare, u.a. mit kritischem Hinweis auf Unklarheiten bezüglich des *Alliierten Vorbehaltsrechts*

[Die weiteren umfangreichen juristischen Fragen/Antworten wurden kaum kommentiert.]

... und die (lange) E-mail eines GI-Mitglieds:

„ .....

... Eine „Affäre“ ist das nicht. Es ist ein Skandal.

Unwürdig ist, dazu zu schweigen.

Als GI-Mitglied und als Bürger fordere ich Sie,
die Autoren und Redakteure, auf, Ihrer gesellschaftlichen Verantwortung, insbesondere die durch Ihre Fachkenntnis gegeben ist, gerecht zu werden.

... „

Resümee

zur „FAQ-Liste zur Überwachungsaffäre 2013“

- *Tenor der Liste:* „NSA kann alles, auch Verschlüsselung knacken“
- Kommentare scheinen i.d.R. von Informatikern zu stammen, meist konstruktiv
- *Tenor der Kritik:* „zu schwammig, unpräzise, unpolitisch, ohne klare Positionierung“
- *Verschlüsselung* stößt bei weitem auf das größte Interesse, und von der GI wird mehr dazu erwartet
- Solche FAQ-Listen müssten *gepflegt* werden – kann die GI so etwas überhaupt leisten?

Kampagne zur E-Mail-Verschlüsselung?

Ein persönlicher Bericht

Kann die GI **handeln** statt nur zu informieren?

Kann sie auf die **Politik** einwirken?

Kann sie dem Bürger **Hilfe zur Selbsthilfe** leisten?


KS 13
Und wenn da die NSA jetzt mitliest?!
Dann verschlüsseln wir es eben!


Aber Frau Merkel hilft da nicht
Dann helfen wir uns eben selbst

Technische Wunschliste:

- *Ende-zu-Ende-Verschlüsselung*
- *einfach* zu benutzen („automatisch“)
- *einfach* einzurichten („one-click installation“)
- *sicher* („vor flächendeckender Überwachung“)
- *kostenlos*

22. August: Rudolf Bayer (TU München) auf der GI-Website:
„E-Mail-Verschlüsselung: ein Selbstversuch und eine Anleitung“

2. Oktober: Pressemitteilung *„GI empfiehlt Verschlüsselung“*
mit Ankündigung konkreter Aktionen (und Verweis auf FAQ-Liste)

24. Oktober: Pressemitteilung *„Abhörskandal erreicht Telefon der Bundeskanzlerin“* (mit Verweis auf FAQ-Liste)

8. November: Sitzung des PAK: Plädoyer für Verschlüsselungs-Kampagne

22. November: Resolution des Fakultätentags Informatik
„Kultur des sicheren Netzes“ mit Appell zur E-mail-Verschlüsselung

Initialzündung durch *R. Bayer*, TU München:

22. August auf Website der GI:
„E-Mailverschlüsselung: ein Selbstversuch und eine Anleitung“
mit Vorschlag zur Verbreitung von *S/MIME:*

- Die Mitglieder der GI installieren die Verschlüsselung ...
- Sie verteilen ihre Zertifikate ...
- Ein Aufruf des Präsidenten der GI an ihre Mitglieder ...
- Ein Aufruf der GI an andere Fachgesellschaften ...
- Die deutschen Fakultätentage folgen der Initiative der GI.
- ... Universitäten, öffentlicher Dienst, Firmen, ...
- Die Einrichtung der Verschlüsselung für E-Mail muss so einfach werden wie das Download und die Installation einer App auf einem Smartphone.

Planung einer „Kampagne“ im PAK:

August: Überlegungen im PAK zur Beförderung eines aktiven GI-Einsatzes für E-Mail-Verschlüsselung

September – Dezember :

PAK erarbeitet konkrete Anleitungen für S/MIME mit Outlook, Mac und Thunderbird

Vorstand:

2. Oktober – Pressemitteilung *„GI empfiehlt Verschlüsselung“:*

„Als Serviceleistung - auch für Nichtmitglieder – wird die GI für das Signieren und Verschlüsseln *Anleitungen* bereitstellen.“

„Als weiteren Schritt ... prüft die GI, inwieweit sie eine einfache und komfortable Lösung zur Erlangung eines vertrauenswürdigen *Zertifikats* anbieten kann ...“

„Dabei sind nicht in erster Linie die Fachinformatiker als Zielgruppe angesprochen ... *sondern alle E-Mail nutzende Bürger*.“

(und Verweis auf FAQ-Liste)

Fakultätentag Informatik:

22. November – Resolution *„Kultur des sicheren Netzes“:*

„Der Fakultätentag Informatik appelliert an seine Mitglieder, in den jeweiligen Fakultäten/Fachbereichen eine *‚Kultur des Sicheren Netzes‘* zu etablieren, die einen hohen Standard an Vertraulichkeit und Integrität persönlicher Daten gewährleistet. Als erster Schritt soll allen Fakultätsangehörigen einschließlich der Studierenden dringend empfohlen werden, E-Mails grundsätzlich zu signieren und zu verschlüsseln, beispielsweise auf Basis der vom DFN ausgestellten Zertifikate.“

(einstimmig angenommen)

Vorstand:

12. Dezember Vorstandssitzung:

- Einführung/Anleitungen sollten sorgfältig getestet und dann ins Netz gestellt werden!
- Damit dann im Januar erneute Pressemitteilung!
- Bei Zertifikaten kann die GI nicht helfen.

(Januar: **neuer Vorstand**)

K.-P. Löhr:

1. Januar: persönlicher Appell und fertige Anleitungen
„*Aufruf zur Verschlüsselung von E-mail*“
auf meiner *privaten* Website im FB Mathematik
und Informatik, FU Berlin

11. März: Aufruf des Dekans an alle Fachbereichs-Mitglieder
„*E-Mail verschlüsseln!*“, mit Verweis auf die Anleitungen
und auf das DFN als Zertifizierungsstelle

25. April: Informationsveranstaltung des Fachbereichs
„*E-Mail verschlüsseln!*“ (S/MIME und OpenPGP)

... und die GI:

1. März: FB Sicherheit bestätigt „Anleitungen sind fehlerfrei“

4. April: PAK-Sitzung (mit Vizepräsident Oberweis):

- Übersichtspapier zu „Grundrecht auf vertrauliche Kommunikation“ machen!
- FAQ-Liste zur E-Mail-Verschlüsselung machen!
- Papier zum Forschungs-, Entwicklungs- und Innovationsbedarf bei der Einführung von verschlüsselter E-Mail machen!

Verschlüsselung für alle!

Alle sind entsetzt über Snowdens Enthüllungen

– aber niemand* verschlüsselt

- meine Familie nicht
- meine Freunde nicht
- meine Studenten nicht
- meine Kollegen zögerlich
- die GI zögerlich
- Ärzte, Rechtsanwälte, Politiker!, ... kaum
- Wirtschaft unterschiedlich

* 6% nach BITKOM-Studie (Juli 2013!) http://t3n.de/news/bitkom-datenschutz-studie-483013/

Alle sind entsetzt über Snowdens Enthüllungen

– aber niemand verschlüsselt – warum?

- „Die *Politik* muss unsere Grundrechte sichern“
- „ich habe ja nichts zu verbergen!“
- „ich weiß nicht, wie das geht!“
- „ist zu umständlich!“
- „ist nicht frei von Stolperstellen“
- „aber S/MIME und PGP sind nicht kompatibel“
- „die NSA knackt es ja doch!“
- „ja, ja, mache ich demnächst“

Bürgerrechte, die man nicht wahrnimmt, sind in Gefahr:

Wahlrecht
„Warum soll ich immer wählen gehen?“
„Weil Demokratie auf Dauer nur dann zuverlässig funktioniert, wenn alle das tun.“

Recht auf Vertraulichkeit der Kommunikation
„Warum soll ich immer verschlüsseln?“
„Weil Demokratie auf Dauer nur dann zuverlässig funktioniert, wenn flächendeckendes Ausspähen unmöglich ist.“

„Without the right to privacy, there is no real freedom of speech or freedom of opinion, and therefore, there is no actual democracy“.

Hat die Politik verstanden?

Katharina Nocun (Piraten):
"Es gibt Dinge, die würde ich auch auf Postkarten schreiben. Für alles andere nutze ich Verschlüsselung.“

Konstantin von Notz (Grüne):
"Das ist so, als wenn Sie den Leuten sagen: Es ist giftiges Fleisch im Umlauf, aber ihr habt ja gute Testgeräte, mit denen ihr vorher die Nahrung testen könnt."
Das sei alles andere als verbraucherfreundlich und werde ohnehin von 95 Prozent der Nutzer nicht angenommen.

http://www.golem.de/news/e-mail-verschluesselung-keine-liebe-auf-den-zweiten-blick-1308-100902.html

Der Innenminister am 14.8.2013:

Auf die Einführung zertifikatsbasierter E-Mail-Verschlüsselung hat das Bundesinnenministerium bislang verzichtet –

> *"aufgrund der damit verbundenen organisatorischen Implikationen, zum Beispiel im Zusammenhang mit der Integration und dem Betrieb einer geeigneten Public-Key-Infrastruktur".*

http://www.golem.de/news/e-mail-verschluesselung-keine-liebe-auf-den-zweiten-blick-1308-100902.html

Konkrete Utopie:
flächendeckende E-mail-Verschlüsselung

Wann gibt es in Deutschland eine Kampagne dafür?

Welche technische Stoßrichtung?

Wer beteiligt sich an einer solchen Kampagne?

Wie wird sie durchgeführt?


KS 13
Und wenn da die NSA jetzt mitliest?!
Dann verschlüsseln wir es eben!