erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Stefan Hügel

Betrifft: Cyberpeace

Vertrauen und Abwehr

Unsere Gesellschaft basiert auf Vertrauen, diese Bedeutung hat Niklas Luhmann (1968) bereits lange vor dem Siegeszug des Internets herausgearbeitet. Nach Luhmann ist Vertrauen notwendig, um die soziale Komplexität unseres Umfeldes zu reduzieren. Nur so können wir die große Zahl an Entscheidungen treffen, die uns die Realität täglich abverlangt – ohne Vertrauen würde diese Zahl ins unermessliche wachsen, bis wir nicht mehr in der Lage wären, damit umzugehen. Bruce Schneier stellt das an einer Alltagssituation plastisch dar:

> *„Just today, a stranger came to my door claiming he was here to unclog a bathroom drain. I let him into my house without verifying his identity, and not only did he repair the drain, he also took off his shoes so he wouldn't track mud on my floors. When he was done, I gave him a piece of paper that asked my bank to give him some money. He accepted it without a second glance. At no point did he attempt to take my possessions, and at no point did I attempt the same of him. In fact, neither of us worried that the other would. My wife was also home, but it never occurred to me that he was a sexual rival and I should therefore kill him."* (Bruce Schneier 2012)

Wenn wir das Internet nutzten, bauten viele von uns dabei bisher ebenfalls auf Vertrauen auf. Wir nutzten bedenkenlos Web-Dienste, die wir für vertrauenswürdig hielten, und verließen uns dabei auf unsere Intuition. Wir verzichteten häufig darauf, Web-Seiten verschlüsselt aufzurufen, da wir darauf vertrauten, dass niemand unsere aufgerufenen Seiten mitliest. Wir verzichteten auch auf Verschlüsselung unserer E-Mail-Korrespondenz, auch bei vertraulichen Dokumenten – es würde schon keiner mitlesen, und wenn, was sollte schon passieren?

Häufig tun wir das heute noch.

Uns ist natürlich klar, dass dieser Vertrauensvorschuss ein wenig Optimismus erfordert. Wir wissen schon immer, dass es im Internet Kriminelle gibt – unser intuitives Sicherheitsgefühl halten wir dagegen in der Regel für ausreichend. Manche stellen irgendwann fest, dass das zu optimistisch war, aber, hey, das sind Ausnahmen, *mir* kann das nicht passieren. Vertrauen wird zur Vertrauensseligkeit.

Auch der Vertrauensvorschuss, den wir unserem eigenen Staat entgegenbrachten, war optimistisch, wir hätten es wissen müssen. Wir wissen in Deutschland nach zwei Diktaturen, dass eine freie Demokratie keine Selbstverständlichkeit ist. Zumindest in der Bundesrepublik hatte sich eine stabile Demokratie herausgebildet – aber auch deren Behörden missbrauchen unser Vertrauen seit Anbeginn, Josef Foschepoth (2012) hat darauf hingewiesen. Ständige Angriffe von politischer Seite auf Vertraulichkeit und Integrität unserer Kommunikation hätten uns ebenfalls warnen müssen. Genannt sei hier nur die Vorratsdatenspeicherung – eine Maßnahme, die vom Bundesverfassungsgericht und vom Europäischen Gerichtshof zurückgewiesen wurde, aber deren Notwendigkeit, ungeachtet solcher Nebensächlichkeiten, immer wieder gebetsmühlenartig betont wird.

Berechtigt war das Vertrauen also wohl nie, heute ist es zerstört. Die Enthüllungen von Edward Snowden (z. B. in Glenn Greenwald 2014) haben sehr deutlich gemacht, dass unsere Kommunikation umfassend überwacht und diese Überwachung immer weiter perfektioniert wird. Diese Überwachung wird parlamentarisch untersucht, in Deutschland vom *1. Untersuchungsausschuss*, genannt *NSA-Untersuchungsausschuss*, der inzwischen *BND-Untersuchungsausschuss* genannt werden müsste, und den weiteren Gremien des Deutschen Bundestags zur Kontrolle der Geheimdienste. Vergleichbare Einrichtungen gibt es in den USA. Doch es zeigt sich, dass seine Arbeit behindert, Information zurückgehalten, und – folgt man den letzten Medienberichten – auch ihm gegenüber gelogen wird. Inzwischen wird darüber berichtet, dass der Bundesnachrichtendienst ausländischen Diensten dabei geholfen haben soll, gegen deutsche Unternehmen Wirtschaftsspionage zu betreiben; eigentlich ist das kaum zu glauben. Erste Strafanzeigen, auch von großen Wirtschaftsunternehmen, sind bereits angekündigt.

Doch in der Online-Ausgabe der *Frankfurter Allgemeinen Zeitung* lesen wir dazu:

> *„Die Spionage der Vereinigten Staaten in unserer Wirtschaft ist gerechtfertigt, in unserem Interesse und keine Industriespionage. Deutschland ist nun einmal einer der großen Exporteure von Rüstungsgütern, sicherheitskritischen Komponenten und Infrastrukturen nach Russland,*

China und in den arabischen Raum. Wir brauchen diese Exporte leider. Sie sind Teil unseres Wohlstands, unseres Systems und unserer Stärke und Stabilität in Europa. Aber sie sind auch gefährlich. Wir verkaufen schwierigen Kräften bessere Handlungsmächtigkeit. Das kann furchtbare Konsequenzen haben." (Sandro Gaycken 2015)

Wir fassen zusammen:

- Um unseren Wohlstand zu sichern, müssen wir Waffen in alle Welt exportieren.
- Damit stärken wir (auch) Regime, die zu unseren Gegnern werden können.
- Um dies wieder „einzufangen", müssen wir die Spionage der US-Amerikaner akzeptieren (und sogar dankbar dafür sein).

Was auf den ersten Blick wie eine gelungene Satire wirkt, ist wohl ernst gemeint. Es gibt Einblick in eine verquere Logik von Militär und Wirtschaft.

Solchen Institutionen blind zu vertrauen, ist offensichtlich naiv und gefährlich. Doch damit gefährden wir auch die Grundlage unserer Gesellschaft. Ohne Vertrauen funktionieren weder Gesellschaft, noch Wirtschaft, noch Politik.

Was tun?

Grundsätzlich gibt es zwei Möglichkeiten, mit der Situation umzugehen:

1. Wir müssen das Vertrauen wiederherstellen.
2. Wir müssen uns selbst schützen und gegen mögliche Angriffe absichern.

Beginnen wir mit dem zweiten Punkt: *„Hilf Dir selbst, sonst hilft Dir keiner"*, das ist das Credo des Neoliberalismus. Das wäre *Victim Blaming*, würden vielleicht andere ausrufen. Doch offensichtlich müssen wir unsere Absicherung selbst in die Hand nehmen. Auch Privatpersonen sollten sich um den Schutz ihrer Kommunikation kümmern. Wie das geht, zeigt zum Beispiel Karin Schuler (2014).

Unternehmen und Behörden schützen sich, indem sie Informationssicherheits-Managementsysteme implementieren und Ihre Systeme technisch und organisatorisch gegen Angriffe von außen und innen absichern. Hier gibt es, besonders bei sicherheitskritischen Systemen, ständigen Handlungsbedarf, um mit den Angreifern Schritt zu halten; manche Organisationen haben vielleicht auch Defizite, die sie zunächst ausgleichen müssen.

Technische Maßnahmen zur Absicherung können sein:

- Verschlüsselung von E-Mails,
- Verschleierung der Metadaten, zum Beispiel im TOR-Netzwerk,
- Härtung von Anwendungen und Infrastruktur,
- Einsatz von Firewalls und Protokollierung von Angriffen,
- Speicherung von Kommunikationsdaten auf Vorrat.

Wait, what? Aber ja doch, die Vorratsdatenspeicherung ist aus Sicht von Sicherheitsbehörden eine technische Maßnahme zur Absicherung der Kommunikation gegen Cyberangriffe und Kriminalität. Auch hier geht es um Vertrauen – das Vertrauen des Staats gegenüber seinen Bürgerinnen und Bürgern. Und es geht um unsere Grundrechte. Unsere Stellungnahme zum IT-Sicherheitsgesetz und die darauffolgende Debatte zeigen, dass hier eine klare Grenze gezogen werden muss (dazu Ingo Ruhmann 2015).

Allein auf Absicherung zu setzen, greift offensichtlich zu kurz. Es ist der Beginn einer Rüstungsspirale im Cyberspace, bei der Angriffs- und Abwehrmaßnahmen auf allen Seiten immer weiter verfeinert werden – NSA-Programme wie BULLRUN zur Entschlüsselung verschlüsselter Kommunikation zeigen das.

Und: Es ist der zum Scheitern verurteilte Versuch, ein soziales Problem technisch zu lösen. Bruce Schneier bringt es erneut auf den Punkt:

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." (Bruce Schneier 2000)

Damit kommen wir zu Punkt 1: Wir müssen das Vertrauen wiederherstellen. Für *Cyberpeace* bedeutet das: Wir müssen darauf vertrauen können, dass potenzielle Gegner uns nicht angreifen. Wir müssen eine strukturelle Nichtangriffsfähigkeit schaffen.

Dazu benötigen wir als erstes Transparenz. Nicht die Form der totalen Transparenz, die die Geheimdienste schaffen wollen, und die Byung-Chul Han kritisiert, wenn er behauptet:

„Die gegenseitige Transparenz kann … allein durch permanente Überwachung erreicht werden, die eine immer exzessivere Form annimmt. Das ist die Logik der Überwachungsgesellschaft." (Byung-Chul Han 2012)

Und:

„Das Vertrauen, das freie Handlungsräume hervorbringt, kann nicht einfach durch die Kontrolle ersetzt werden." (Byung-Chul Han 2012)

Dennoch benötigen wir sie: als Nachvollziehbarkeit politischer Entscheidungen, als Nachvollziehbarkeit der Arbeitsweise von Organisationen, als Nachvollziehbarkeit technischer Systeme. Es muss kontrolliert werden können, wie militärische und geheimdienstliche Organisationen arbeiten – wenn nicht durch die Öffentlichkeit, dann zumindest durch ein gestaffeltes System vertrauenswürdiger Instanzen. *„Die Menschen müssen ihrem Herrscher glauben und vertrauen"*, zitiert Han *Richard Sennett* (2004) – aber das hat offensichtlich nicht funktioniert, auch wenn die Bundesregierung das gerne glauben machen will.

Wir müssen als Gesellschaft in der Lage sein, zu beurteilen, wie es zu politischen Entscheidungen in unser aller Namen kommt. Politische Prozesse müssen in der Öffentlichkeit stattfinden,

ohne dabei Rückzugsräume für Unfertiges völlig zu verschließen. Technische Systeme müssen quelloffen sein, und dabei dennoch legitime Interessen an Geschäftsgeheimnissen wahren. Doch Rückzugsräume und Geschäftsgeheimnisse dürfen nicht dazu missbraucht werden können, Fehlverhalten zu vertuschen. Die Grenze ist nicht leicht zu ziehen und sie bedarf eines gesellschaftlichen Konsenses. Wir haben diese Regierung gewählt, sie handelt in unserem Namen, wir tragen für ihr Handeln eine (Mit-) Verantwortung.

Letztlich wird es ohne Vertrauen nicht gehen. Doch die Institutionen, denen wir vertrauen sollen, müssen sich dieses Vertrauens würdig erweisen. Die Medienberichte der vergangenen Tage, Wochen und Monate zeigen, dass dafür viel zu tun ist.

Referenzen

Josef Foschepoth (2012): Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. Göttingen, Bristol: Vandenhoek & Ruprecht

Sandro Gaycken (2015): Spionage? Kein Grund zur Aufregung! Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/politik/inland/bnd-affaere-spionage-unter-freunden-kein-grund-zur-aufregung-13564435.html

Glenn Greenwald (2014): Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München: Droemer

Byung-Chul Han (2012): Transparenzgesellschaft. Berlin: Matthes & Seitz

Niklas Luhmann (1968): Vertrauen. 4. Auflage 2000. Stuttgart: Lucius & Lucius

Ingo Ruhmann (2015): Schutz von Grundrechten nicht in Sicht. FIfF-Kommunikation 1/2015, Seite 10

Bruce Schneier (2000): Secrets & Lies. Digital Security in a Networked World. Indianapolis: John Wiley & Sons

Bruce Schneier (2012): Liars & Outliers. Enabling the Trust that Society needs to Thrive. Indianapolis: John Wiley & Sons

Karin Schuler (2014): Wer nicht kämpft, hat schon verloren. FIfF-Kommunikation 1/2014, Seite 34

Richard Sennett (2004): Respekt im Zeitalter der Ungleichheit. Berlin: Berliner Taschenbuch-Verlag

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faires Silber.

Ach, die EU. Hauptsache der Euro rollt. Die USA hatten ein Gesetz zur Regulierung von Geschäften mit Konfliktmineralien geschaffen, das nicht perfekt war, aber innovativ und anspruchsvoll. Die EU wollte nachziehen, was die Kommission aber vorlegte, war schwach: Während in den USA alle börsennotierten Endproduktanbieter – also all die Apples, HPs, Ciscos und Intels, die wir kennen – Berichtspflichten auferlegt bekommen haben, sollen in der EU nur die paar Rohstoffimporteure berichten, die niemand kennt, und noch schlimmer: nur wenn sie wollen, denn verpflichtend soll es auch nicht sein. Die Hoffnung der Zivilgesellschaft – auch das FIfF war Teil dieser NGO-Koalition – ruhte daher auf dem EU-Parlament. Das Komitee für Entwicklungspolitik des Parlaments stimmte für eine verbindliche Berichtspflicht. Federführend ist aber leider das Parlamentskomitee für Internationalen Handel, und das hat den Kommissionsentwurf ohne viele Änderungen durchgewunken und Mitte Mai dem gesamten Parlament zur Abstimmung vorgelegt.

Im EU-Parlament war die Stimmung dann jedoch eine ganz andere. In einer kaum für möglich erscheinenden Wende wurde nun ein Gesetzentwurf geschmiedet, der sogar über das hinaus geht, was in den USA verlangt wird: Importeure müssen sich von der EU zertifizieren lassen, und alle Hersteller, die diese Rohstoffe in ihren Produkten haben – in der EU immerhin gut 800 000 meist mittelständische Unternehmen – müssen ihre Sorgfaltspflicht nachweisen, und das nicht nur für Zentralafrika, sondern für alle (noch zu definierenden) Konfliktgebiete. Vielleicht hat ja das Lobbying der vielen NGOs doch gefruchtet? Als nächstes muss das Gesetz allerdings durch den Europäischen Rat, wo es bestimmt wieder abgeschwächt wird.

In den USA steht unterdessen bald schon die zweite Runde der Pflichtberichte an, diesmal für die Geschehnisse im Jahr 2014. Überrascht hat Apple, denn sie veröffentlichten ihren Bericht schon im Februar. Die anderen dann wohl wieder kurz vor knapp. Amnesty International und Global Witness haben sich die letztjährigen Berichte angeschaut und mussten feststellen: Fast 80 % der Unternehmen haben sich gar nicht vollständig an die Vorgaben gehalten und klagen lieber dagegen. Ach, die Multis. Hauptsache der Dollar rollt.

Samsung bleibt von all dem befreit, da aus Südkorea. Aber sie sollten schauen, was in Taiwan mit RCA passierte: Der inzwischen Thomson Multimedia gehörende US-Veteran muss über 30 Jahre, nachdem Mitarbeiter Belastungen durch Chemikalien im Herstellungsprozess ausgesetzt waren, einige Millionen Entschädigung zahlen. Dem versucht Samsung, um auf diesen aktuellen Hersteller von LCDs, CPUs u.v.a. zurück zu kommen, zuvorzukommen, indem sie freiwillig (und ohne Schuldeingeständnis natürlich) erkrankten Mitarbeitern Gelder in Aussicht stellen, natürlich offiziell nicht als Entschädigung, sondern als Fürsorge für ihre Mitarbeiter. Wir berichteten schon davon; neu ist aber, dass es „*not our final plan*" ist. Da kommt also noch was.

Was gibt es Neues bei den beiden Graswurzelprojekten der fairen Elektronik? Nager-IT möchte, solange es z. B. kein faires Lötzinn gibt – FairLötet ist noch im Entstehen – zum Ausgleich aus dem Verkauf der Mäuse Gelder für ein Unterstützungsprojekt in Indonesien bereitstellen, dort wo vieles des in Elektronik eingesetzten Zinns herkommt, und zwar auf illegale, Gesundheit und Umwelt gefährdende Weise. Außerdem sind die Holzscrollräder