Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)10

Öffentliches Fachgespräch des Ausschusses „Digitale Agenda“ des Deutschen Bundestages zum Thema „IT-Sicherheit“

Schriftliche Stellungnahme von Dr. Sandro Gaycken
Institute of Computer Science, AG Secure Identity
Freie Universität Berlin

Zu den Fragen des Ausschusses nehme ich wie folgt Stellung:

1.1 Inwieweit ist eine sichere Kommunikation über die bestehenden Infrastrukturen aus Ihrer Sicht heute überhaupt noch möglich?

Sicherheit ist relativ. Eine sichere Kommunikation gegen schwache Angreifer (Kleinkriminelle, Aktivisten) ist mit bestehenden Techniken unter akzeptablen Kollateralschäden möglich, sofern diese Techniken dem Stand der Technik entsprechen, agil, effektiv und effizient sind und korrekt implementiert und bedient werden.

Eine sichere Kommunikation gegen starke Angreifer (organisierte Kriminelle, Nachrichtendienste, Militärs) ist gegenwärtig nicht möglich. Das „normale“ Modell der Rechnersicherheit ist diesen Angreifern gegenüber konzeptionell überfordert und überholt. Dieses normale Modell hat sich aus Grundannahmen zur Computersicherheit der Sechziger bis Achtziger Jahre herausgebildet.
Diese waren:

- Computer sind nur in engen Spezialbereichen nutzbar;
- Kritische Abhängigkeiten von IT sind moderat;
- Angreifer sind vorrangig Kleinkriminelle, die vor allem über das Internet angreifen;
- Angreifer sind statisch und wenig innovativ;
- Systeme sind isolierbar, Perimeter lassen sich einziehen und kontrollieren;
- Systeme sind nur kompliziert, nicht komplex;
- Systeme sind streng hierarchisch und geordnet;
- Systeme sind verständlich;
- Systemeigenschaften sind prüfbar;
- Fehlverhalten ist erkennbar;
- Angreifer sind erkennbar;
- Systeme sind über ausgewählte Vektoren kontrollierbar;
- Hersteller sind vertrauenswürdig;
- Restrisiken sind tolerabel.

Das resultierende normale Modell hat eine grundlegend verwundbare Informationstechnik akzeptiert, da diese in den wenigen kritischen Kontexten für isolierbar und vertrauenswürdig gehalten wurde, während man in nicht-kritischen Kontexten die wenig gefährlichen Angreifer mit vorrangig reaktiven ad

hoc Sicherheitstechnologien an Übergangspunkten eines Perimeters kontrollieren konnte.

Dieses Modell wurde über fünfzig Jahre lang verfolgt und hat die Innovationsmechanismen angetrieben. Da Sicherheit als Design-Merkmal in IT zudem schwierig und teuer ist und wichtigeren Merkmalen wie Time-To-Market, Geschwindigkeit, Volumen und Multifunktionalität entgegenwirkt, wurde sie in diesem Prozess nicht nur nicht verbaut, sondern oft noch weiter geschwächt und verschlechtert, wobei sogar Standards in Richtung Unsicherheit aufgeweicht wurden, wie die Standards des „Orange Book“[1] des US Department of Defense aus dem Jahre 1983 in die wesentlich weicheren „Common Criteria“[2]. So wurde IT im Wesentlichen stark unsicher entwickelt, während Sicherheit als Zusatzaufgabe externalisiert wurde.

Mit der Zeit allerdings sind mit dem Wachstum der Funktionalität auch die ökonomischen Interessen an der IT, vor allem an vernetzter IT, stärker gewachsen, so dass inzwischen breite und kritische strategische und ökonomische Abhängigkeiten von diesen Technologien entstanden sind. Dies führt nun einerseits zu einer Diversifikation der bestehenden kleinkriminellen Geschäftsmodelle, vor allem aber zum Aufkommen neuer Angreifer wie organisierter Krimineller und fremder Staaten, die jetzt ein reiches, wirtschaftlich wie strategisch interessantes Target Set vorfinden. Durch diese jüngere parallele Entwicklung von IT und neuen Angreifern sind die Grundannahmen des normalen Modells der IT-Sicherheit umgekehrt.
Die aktuellen Bedingungen sind:

- Computer sind überall – fast alle kritischen Prozesse sind mit IT durchzogen;
- Abhängigkeiten sind hochkritisch – ohne die IT sind die Prozesse nicht länger durchführbar, was häufig noch Kaskadeneffekte auf dahinterliegende, eng gekoppelte Prozesse nach sich zieht;
- Angreifertypen sind heterogenisiert, mit vielen neuartig starken Akteuren – das Spektrum der Angreifer ist deutlich erweitert um organisierte Kriminelle, Nachrichtendienste und Militärs verschiedenster Länder mit unterschiedlichsten Motivationen und Fähigkeiten;
- Angreifer sind dynamisch und hochinnovativ – die neuen, starken Angreifer verpflichten in der Regel die besten verfügbaren Experten für Angriffe, eingeschlossen Wissenschaftler und Firmen, so dass deren Angriffe in der Regel vollständig informiert sind und der Defensive konstant nicht nur einige Monate, sondern einige Jahre voraus sind;
- Systeme sind nicht isolierbar, Perimeter sind nicht mehr effektiv – viele kritische Systeme sind inzwischen an große externe Netzwerke oder sogar an das Internet angeschlossen. Zudem greifen die neuen Angreifer die IT-Sicherheitsumgebung mit an und nutzen bevorzugt unkonventionelle Vektoren wie manipulierte Hardware und Software oder Innentäter, so dass

[1] http://csrc.nist.gov/publications/history/dod85.pdf
[2] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/commoncriteria_node.html

Perimeter irrelevant werden. Selbst entnetze Systeme – wenngleich deutlich schwerer und teurer anzugreifen – können nicht mehr als isoliert gelten;

- Systeme sind komplex, nicht kompliziert – IT-Systeme produzieren Effekte, die von ihren Entwicklern und Operateuren nicht antizipiert werden können[3];
- Systeme sind "Spaghetti"-Konstrukte – in den meisten IT-Produkten gibt es keine klare Ordnung, wenig Dokumentation und keine Segregationen, so dass die Systeme undurchsichtig werden und Angreifern viele Interaktionen ermöglichen;
- Systeme sind nicht länger verständlich – die hohe Komplexität aktueller Systeme macht es selbst Experten inzwischen unmöglich, die Systeme und ihr Verhalten vollständig zu modellieren und zu antizipieren. IT-Systeme sind von technischen Konstrukten zu Naturgegenständen geworden;
- Systemeigenschaften sind nur begrenzt prüfbar – infolge der Komplexität;
- Fehlverhalten ist kaum erkennbar – aktuelle Systeme zeigen eine hohe Verhaltensvielfalt mit einem hohen „Grundrauschen", was ein Erkennen vorsichtig konstruierten Fehlverhaltens sehr schwer macht. Auch „Big Data" Analysen können effizient getäuscht werden;
- Angreifer sind kaum erkennbar – starke Angreifer sind von den marktgängigen Technologien der Detektion nicht erkennbar. Von den 231 Operationen des US-Cybercommand aus dem Jahr 2011 (nach einem Snowden-Dokument[4]) wurde lediglich eine einzige entdeckt (die Spionage-Operation „Flame"[5]), was repräsentativ für das Verhältnis Hellfeld zu Dunkelfeld in diesem Bereich sein sollte. Chinesische Angreifer sind eine Ausnahme. Sie sind oft trotz eines vermuteten starken Hintergrunds leicht erkennbar, was jedoch daran liegt, dass sie sich keine Mühe zur Tarnung geben und sehr viele Ziele angreifen. Zudem tendieren starke Angreifer dazu, die Security- und Safetyprodukte eines Ziels mit anzugreifen. Dies geschah etwa im Kontext von Stuxnet und wird auch durch die sogeannten „Shopping List" der ANT Division der NSA[6] aus den Snowden Dokumenten klar belegt. Dort sind diverse Angriffe auf gängige Firewalls und andere Sicherheitstechnologien aufgelistet. Viele der Techniken sind zudem „Persistence Operations", die dazu dienen, einen Angreifer dauerhaft und unerkennbar in einem System zu halten;
- Systeme müssen systemisch kontrolliert werden – starke Angreifer können überall angreifen;
- Hersteller sind kompromittiert – die Snowden Dokumente haben den schon lange bestehenden Verdacht erhärtet, dass viele Hersteller und Standardprodukte von Nachrichtendiensten unterwandert sind und gezielt

[3] Siehe Perrow, „Normale Katastrophen. Die unvermeidlichen Risiken der Großtechnik", Frankfurt 1987/1992

[4] http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html

[5] http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

[6] http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/

eingebaute Schwachstellen beherbergen. Beispiele hier waren RSA, Huawei, BELGACOM, wobei aufgrund der hohen Summe von 652 Millionen US-Dollar, die im Rahmen des „Project GENIE“[7] für den Einbau solcher Schwachstellen in Kernprodukte von einer konsequenten und nachhaltigen Verseuchung fast aller Produkte des kommerziellen Marktes mit hoher Verbreitung ausgegangen werden sollte. Auch andere Nachrichtendienste und organisierte Kriminelle dürften diese Option genutzt haben, da das Risiko gering ist und die Effizienz sehr hoch;
- Restrisiken sind zu hoch und nicht tolerabel.

Mit diesem durchgreifenden Wandel der Basisbedingungen der IT-Sicherheit muss das normale Modell der IT-Sicherheit dringend hinterfragt werden. Da die klassischen Techniken der reaktiven ad hoc Sicherheit (wie reaktive Filter, Detection und Prediction Techniken, Intrusion Mangement, Security Operation Center etc.) nicht länger funktionieren und als konzeptionell defizitär angesehen werden müssen, müssen die Verwundbarkeiten, die kritischen Sicherheitslücken der darunter liegenden und bislang als verwundbar tolerierten Informationstechnologien behoben werden.

Dies ist allerdings unmöglich, da ein großer Teil dieser Verwundbarkeiten nicht auffindbar ist. Selbst nach umfangreichen Analysen und Tests sind etwa 0,004% (in gehärteten und nie veränderten Open Source Kernmodulen) bis 1% (bei schlecht entwickelter Software) des Codes, geschätzt nach Zeilen Code, kritische Sicherheitslücken, bei denen voller und oft persistenter Systemzugang ermöglicht wird. Aufgrund der hohen Menge Code ergibt dies für die meisten Hardware- und Softwareprodukte bereits unkontrollierbar große Menge auszubeutender Sicherheitslücken. Zudem sind weitere Angriffe über ad hoc Bedeutungsveränderungen möglich, die aufgrund des turing'schen Halteproblems prinzipiell immer möglich sind, sowie über andere Vektoren wie die Supply Chain und Innentäter.

Dies ergibt für viele Basistechnologien viele tausend kritische Sicherheitslücken – ein Umstand, der auf Cybersicherheitskonferenzen gerne ausgespart und umschifft wird. Betriebssysteme beherbergen bis zu einigen zehntausend kritische Sicherheitslücken, einzelne Applikationen haben einige hundert bis einige tausend Sicherheitslücken (dies gilt auch für Open Source Projekte mit niedriger Entwicklerdichte und hoher Modifikationsrate) und auf Prozessoren lässt sich nicht verifizieren, dass keine absichtlichen Schwachstellen oder Switches verbaut sind.

Besonders besorgniserregend sind hochkomplexe Datenbanksysteme für Geschäftsprozesse, zu denen hohe Abhängigkeitsbeziehungen bestehen und die aufgrund ungewöhnlicher Größe, sehr hoher Komplexität, fehlender Segregation und schlechter Security-, Patching- und Entwicklungspraxis bis zu einigen hunderttausend kritische Sicherheitslücken aufweisen[8]. Vor diesem Hintergrund

[7] http://leaksource.info/2013/08/31/codename-genie-nsa-to-control-85000-implants-in-strategically-chosen-machines-around-the-world-by-year-end/
[8] Siehe dazu etwa virtualforge.com

ist auch der Plan der Einführung solcher Systeme für die Führungsunterstützung der Bundeswehr als zweifelhafte Entscheidung zu bewerten.

Der Kollaps der Annahmen des normalen Modells hat gegenwärtig innerhalb kurzer Zeit eine dramatische Veränderung der Sicherheitslage herbeigeführt. Aktuelle Informationstechnik muss gegenüber starken Akteuren als zutiefst unsicher bewertet werden, die Effizienz konventioneller IT-Sicherheit – auch wenn diese unter neuen Begriffen vermarktet wird – als fragwürdig und ungeprüft.

1.2 Welche Erkenntnisse gibt es zu den Angriffsmöglichkeiten und Kompromittierungen der Informations- und Kommunikationsinfrastruktur (Hard- und Software, Netzwerktechnik, Normen und Standards etc.)?

Wie bereits erwähnt haben insbesondere die größeren Angriffe und Spionagekampagnen der letzten Zeit sowie die Dokumente Edward Snowdens deutlich nachgewiesen, dass starke Angreifer alle Teile der Informationstechnik unabhängig von Schutzperimetern angreifen können. Hard- und Software – Betriebssysteme, Firmware wie Applikationen – sind inhärent unsicher und oft noch mit zusätzlichen Schwachstellen versehen. Netzwerktechniken sind ebenfalls weitgehend unsicher. Hier stehen verschiedene Optionen zur Verfügung. Angreifer können mit den Providern kooperieren oder diese per Gesetz zur Kooperation zwingen. Sie können bei den Providern einbrechen (geschehen bei BELGACOM durch die GCHQ[9]). Sie können über verwundbare Teile angreifen wie bei Krypto-Telefonen über die Hardware[10] oder über hochgradig verwundbare Basisstrukturen in den Telekommunikations-Backbones wie den auch in Deutschland vorzugsweise genutzten Huawei-Routern, die nach Meinung unabhängiger Sicherheitsforscher ungewöhnlich viele kritische Schwachstellen aufweisen[11]. Auch Normen und Standards sind als schwierig zu erachten, da diese durch sicherheitsfeindliche Interessen der IT-Industrie über die Jahre aufgeweicht und geschwächt wurden und zudem teilweise von Nachrichtendiensten unterwandert sein sollen, wie etwa John Gilmore aus Sitzungen der Krypto-Arbeitsgruppen in US-amerikanischen Standard-Komitees berichtet[12].

1.3 Welche Maßnahmen (auch gesetzgeberische) müssen ergriffen werden, um den Grundrechtsschutz und die Vertraulichkeit der Kommunikation wieder herzustellen?

Soll eine hohe Vertraulichkeit und Gewährleistung der Sicherheit der

---

[9] http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

[10] http://www.berkes.ca/archive/berkes_hardware_attacks.pdf; sowie Becker, Regazzoni, Paar, Burleson, „Stealthy dopant-level hardware trojans“, in: Proceeding CHES'13 Proceedings of the 15th international conference on Cryptographic Hardware and Embedded Systems, 2013

[11] http://www.cnet.com/news/expert-huawei-routers-are-riddled-with-vulnerabilities/

[12] http://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html

Kommunikation wieder hergestellt werden, die auch gegen gezielte Aktivitäten starker Akteure schützt, muss die aktuelle IT neu entwickelt werden, nach entsprechend hohen Standards wie etwa im bereits genannten Orange Book definiert.[13] Nicht verifizierbare Teile wie Hardware müssten unter Hochsicherheitsbedingungen hergestellt werden. Die bestehende IT müsste ersetzt werden. Stark unsichere Teile wie eine der erwähnten Geschäftsprozess-Umgebung müssten weitgehend stark isoliert werden. Die Isolierung stark inhärent unsicherer IT von kritischen Prozessen muss dringend gesetzlich forciert werden. Maßnahmen wie Innentäterabwehr und Supply Chain Sicherheit müssen deutlich erhöht werden.

Geht es nur um eine Abwehr schwacher Angreifer sind inkrementelle Verbesserungen der bestehenden Techniken ausreichend, wobei diese aber durch rigidere Prüfungen ergänzt werden sollten (siehe unten).

Weiche Maßnahmen wie Normen oder „No Spy Abkommen“ sind unsinnig, da die Einhaltung dieser Normen und Abkommen durch die hohe Ineffizienz der Detektion und Identifikation nicht kontrolliert und eingeklagt werden kann. Bei entsprechenden Abkommen ist zudem davon auszugehen, dass diese nicht unterzeichnet werden. Zudem würden allenfalls „like-minded“ Nationen diese Abkommen untereinander unterzeichnen, was zu einem asymmetrischen Verlust an nachrichtendienstlicher Informationsgewinnung und einem strategischen Schaden gegenüber anderen Staaten führt.

Stärker offensive Maßnahmen wie Internet-Überwachung und Vorratsdatenspeicherung oder Rückangriffe und Upstream Intelligence zu Zwecken der Aufklärung sind zwar gegenwärtig zum Teil erfolgreich bei Firmen wie FireEye oder Mandiant[14], umfassen allerdings datenschutzrechtliche und sicherheitspolitische Nebenwirkungen und haben vor allem aufgrund ihrer Erfolge eine stark beschleunigte Gegenentwicklung der Offensive initiiert, die viel Spielraum in dieser Beziehung hat und mit wesentlich erhöhter Tarnung und Täuschung reagieren wird, bis hin zur vorzugsweisen Nutzung sogenannter „False Flag Operationen“[15], bei denen gefälschte Spuren auf einen anderen vermeintlichen Angreifer ablenken und so Eskalationen produzieren. Aufgrund der hohen Unsicherheit von Datenspuren, der bereits jetzt schlechten Effizienz vieler Maßnahmen und der in Zukunft deutlich höheren Möglichkeit von False Flag Angriffen inklusive der davon provozierten Eskalationen sind passive technische Schutzmaßnahmen offensiver Rückverfolgung deutlich vorzuziehen.

---

[13] Siehe hierzu auch: Gaycken, "Back to Basics: Beyond Network Hygiene" (mit Felix Lindner), in: Melissa Hathaway, Best Practices for Computer Network Defence, NATO SPS Publication, Brussels 2014 sowie Gaycken, "Resetting the System – Why High Security Computing Should be a Policy Priority“ (mit Greg Austin), in: EastWest Discussion Papers, New York 2014.

[14] https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/

[15] Siehe Gaycken, „Cyberwar – das Wettrüsten hat längst begonnen“, Berlin 2012

Gesetzliche und politische Maßnahmen sollten folglich vorrangig eine grundlegende Reform der Informationstechnik anstreben.

Im Bezug auf den weiteren Schutz der Grundrechte sind Privatheit und auch die Gewährleistung des Widerstandsrechts nur herstellbar, wenn auf strafrechtlich oder kommerziell motivierte ungezielte Massenüberwachung verzichtet wird und wenn auch die Beforschung, Entwicklung und Produktisierung entsprechender Technologien verboten wird.[16] Hier wäre ebenfalls wünschenswert, eine internationale Ächtung der hocheffizienten Internet-Massenüberwachung zu erreichen, um autoritären Regierungen die Kontrolle ihrer Bevölkerungen über diesen Vektor zu erschweren. Außerdem könnte eine Entwicklung von Gegentechnologien erwogen werden, wie sie durch das US Department of State für anonyme Kommunikation bereits initiiert wurde.

Außerdem ist der Gesetzgeber in der Pflicht, die Beforschung und Entwicklung klarer, unabhängiger und objektiver Risikometriken zu beauftragen, welche grundlegende Verwundbarkeiten von IT sowie die Messung der Effizienz von IT-Sicherheit einschließen und die gegenwärtige Praxis der Zertifizierung ergänzen oder ersetzen.

Dies schließt auch dringend eine kritische Evaluierung der eigenen Ansätze ein. So ist aufgrund einiger Untersuchungen der Universität Cambridge[17] zu erwarten, dass klassischen Schwerpunktthemen des Bundes wie „Sichere Identität“, „IT-Sicherheit für den Bürger“ und „Botnetz-Abwehr“ aus einer aufgeklärten Cyber-Risikoperspektive als deutlich niedrige Risiken oder kostenineffiziente Lösungen bewerten werden dürften, für die bereits zu viel Mittel ausgegeben wurden, während etwa strategische Industriespionage als drastisch höheres Risiko bislang beinahe unbegleitet blieb.

Der Staat muss zudem entsprechende Prüfungen forcieren und „Sicherheitsversager“ aus kritischen Kontexten entfernen.

2. Welche Abwehrmöglichkeiten stehen heute zur Verfügung, um die eigene Datensicherheit in kompromittierten Kommunikationsinfrastrukturen zu erhöhen und welche Möglichkeiten gibt es für den Gesetzgeber, diese auszubauen?

Auf die Frage wurde oben schon weitestgehend geantwortet. Die Relativität der Sicherheit durch die Relation zwischen Angreifer und Opfer ist als Basisorientierung einzuziehen. Dann steht je nach Relation prinzipiell steht eine große Zahl potentieller Abwehrmöglichkeiten zur Verfügung, um die Datensicherheit zu erhöhen. Allerdings sind Effektivität und Effizienz vieler dieser Technologien unklar und insbesondere in Relation zu starken Angreifern umstritten. Der Gesetzgeber sollte hier Entscheidungen erleichtern, indem er es den Betroffenen ermöglicht, Risiken und Produkte unabhängig

[16] Siehe hierzu auch Gaycken, „1984.exe“, Bielefeld 2008; sowie Gaycken, „Jenseits von 1984“, Bielefeld 2013.
[17] Siehe dazu Anderson et al, „Measuring the costs of cybercrime“, WEIS 2012

und nach wissenschaftlichen Maßstäben zu bewerten. Davon ausgehend kann der Gesetzgeber besonders vielversprechende Sicherheitstechnologien fördern. Ohne klare Risiko- und Effizienzmodellierungen sollten keine Förderungen ausgegeben werden. Cybersicherheit muss aufgrund der hohen Kosten und Risiken dringend strategisch auf Basis klarer Zahlen erfolgen. Dies wird gegenwärtig in keiner Weise verfolgt. Zudem müssen Kataloge wünschenswerter Sicherheitsmerkmale und Kriterien sowie Sicherheitshöhen entwickelt werden, im Einklang mit deutschen Vorstellungen von Grundrechten und Datenschutz, die sich an den realen Bedarfen von Gesellschaft, Politik und Wirtschaft orientieren, nicht an den ökonomischen Interessen etablierter Hersteller oder den akademischen Forschungsinteressen der Techniker.

3. Welche Maßnahmen können Anbieter/Betreiber von Kommunikationsdiensten und –infrastruktur ergreifen und welche Möglichkeiten gibt es für den Gesetzgeber, die hierbei zu unterstützen?

Wie oben bereits angedeutet, sollten Anbieter und Betreiber vor allem zu einer hohen Sicherheit der eigenen oder der selbst verwendeten Produkte angehalten werden. Dies erfolgt gegenwärtig nicht in verantwortlicher Weise. Daher ist der Gesetzgeber vor allem zur Kontrolle der Basissicherheit der Techniken der Anbieter und Betreiber angehalten. Davon abgesehen gibt es eine Reihe von Maßnahmen, die Anbieter und Betreiber realisieren können, um eine relative Erhöhung von Sicherheit zu erreichen. Eine hinreichend starke Verschlüsselung aller Kommunikation etwa ist eine gute und effiziente Maßnahme, um fremden Nachrichtendiensten das Interesse an einer Massenüberwachung auszutreiben. Eine massenhaften Entschlüsselung liegt außerhalb der Betriebsrationalität der Nachrichtendienste.

Ebenfalls überaus sinnvoll ist das sogenannten „Schengen-Routing“. Dies liefert zwar keine Sicherheit vor gezielten Angriffen durch Nachrichtendienste, stellt allerdings für Daten eine klare Territorialität her, so dass eventuelle gezielte Einbrüche und ähnliche Aktivitäten fremder Nachrichtendienste und datenverwertender Unternehmen klar kriminell wären. Damit ist zumindest von einem sinkenden Interesse der Dienste und Unternehmen auszugehen, da die Verwertbarkeit der Daten reduziert wird und da massenhafte Datendiebstähle leicht detektierbar wären und Klagen und Eskalationen nach sich ziehen könnten.

In diesem Kontext ist noch darauf hinzuweisen, dass auch Verschlüsselung keine verlässliche Sicherheit vor gezielten Angriffen der Nachrichtendienste herstellt. Hier ist in der deutschen Diskussion oft eine Überbewertung der Möglichkeiten der Verschlüsselung als „Allheilmittel“ ln, zum Teil durch mondäne kommerzielle oder politische Interessen der Diskutanten.

Zwar gelten ab 256 Bit nach Advanced Encryption Standard verschlüsselte Inhalte als nicht mit „Brute Force“-Methoden (als maschinellem „Raten“) knackbar, allerdings ist ein gängiges Problem einer Ende-Zu-Ende-Verschlüsselung eben der Umstand, dass das Ende immer noch angegriffen werden kann, was starken Akteuren wie skizziert durchaus offen steht. Dort können diese Angreifer auf Hardware- oder Betriebssystem-Ebene angreifen, wobei jede danach erfolgende Verschlüsselung sinnlos ist (die NSA hat einige Bemühungen für entsprechende Angriffe auf diesen Systemtiefen

unternommen[18]), sie können Muster ablesen, Seitenkanäle angreifen und beobachten oder die für die Verschlüsselung notwendigen Random Number Generator attackieren. Zudem sind auch einige der Algorithmen der Verschlüsselung kritisch auf ihre Wirksamkeit zu betrachten. Bekannt ist etwa, dass die NSA der Elliptic Curve Verfahren unterwandert hat[19] und die über Zwischenhändler auch in Deutschland mit Sicherheitsprodukten präsente Firma RSA dafür bestochen hat[20], diese korrumpierten Verfahren als Default anzuwenden. Außerdem haben Nachrichtendienste teilweise die Entwicklung besonders komplexer Krypto-Standards infiltriert. So ist etwa bei dem auch von der DIN empfohlenen IPSec unklar, ob die NSA in der komplexen Mathematik Fallstricke untergebracht hat. Krypto-Experten wie Bruce Schneier empfanden den Algorithmus als zu komplex für eine rigide und zweifelsfreie Prüfung[21]. Verschlüsselung kann zudem falsch implementiert oder nur mit schwachen Passwörtern gesichert sein.

4. Inwieweit kann die Sicherheit bei der Nutzung von Kommunikationsdiensten wie De-Mail, E-Mail und anderen Messaging-Diensten weiter erhöht werden? Wie werden die bisherigen gesetzlichen Grundlagen hierzu eingeschätzt? Welchen Beitrag können öffentliche Stellen (z.B. Bundesdruckerei, Bundesamt für die Sicherheit in der Informationstechnik) leisten, wenn diese Zertifikate zur Verschlüsselung zur Verfügung stellen?

Die Frage ist weitestgehend bereits beantwortet. Der Einbau einer Vielzahl von zusätzlichen Sicherheitsmaßnahmen wie einer Verschlüsselung kann technisch erfolgen und ergibt eine sinnvolle relative Erhöhung der Sicherheit. Außerdem sollte inländische wie ausländische Unternehmen zu einer strengeren Befolgung deutscher Datenschutzgesetze gezwungen werden, indem sie etwa Daten nicht oder nur unter explizitem Einverständnis der Nutzer ins Ausland leiten (wo sie ausgewertet werden könnten und nicht länger deutschem Recht unterliegen).

Öffentliche Stellen könnten diesen Prozess sinnvoll unterstützen, indem sie insbesondere für Laien verständliche, implementierbare und zuverlässige Verschlüsselungen sowie weitere Sicherheitstechniken anbieten. Außerdem sollten öffentliche Stellen intensiver, neutral und vor allem unabhängig über Schwächen und Risiken aufklären und über die Konsequenzen und Details von Datengeschäften informieren. Zertifikate wären ein guter Schritt in diese Richtung.

5. Wie können Privatpersonen sowie klein- und mittelständische Unternehmen zur stärkeren Nutzung sicherer Kommunikationsverbindungen und Verschlüsselungsverfahren bewegt werden? Besteht hier politischer Handlungsbedarf?

Meines Erachtens besteht hier kein politischer Handlungsbedarf, solange keine direkten, gesellschaftlichen oder volkswirtschaftlichen Schäden zu erwarten sind. Wenn ein

[18] https://www.schneier.com/blog/archives/2014/01/nsa_exploit_of.html
[19] https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html
[20] http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331
[21] https://www.schneier.com/paper-ipsec.html

Privatnutzer seine privaten Daten einem Unternehmen zur Verfügung stellt, da er neben gezielter Werbung keine hohen Kollateralschäden zu erwarten hat – und wenn er dazu von den Interessen und Fähigkeiten der NSA weiß – ist dies eine informierte Entscheidung, die nicht reguliert werden muss. Dennoch sollte umfangreichere Aufklärung über die Volumina privater Daten in kommerzieller Überwachung stattfinden, um entsprechend informierte Entscheidungen zu stützen. Sind die Unternehmen forschende und entwickelnde Firmen, müssen sie deutlich stärkeren Sicherheitsmaßnahmen unterworfen werden, um sie vor ausländischer Industriespionage – der für Deutschland mit Abstand größten Cybergefahr – zu schützen. Hier ist der Staat aus volkswirtschaftlichem Eigeninteresse in der Pflicht, den Unternehmen hocheffiziente Sicherheitstechnologien zu entwickeln und laientauglich implementierbar zur Verfügung zu stellen.

6. Inwieweit besteht politischer Handlungsbedarf zur Verbesserung der Datensicherheit und des Datenschutzes bei neuen Kommunikationsdiensten wie mobilen Instant-Messengern (WhatsApp etc.)?

Der Gesetzgeber muss klarstellen und zur Ermöglichung informierter Entscheidungen bekanntmachen, welche Nutzungsmodelle in welchen Formen und Tiefen hinter entsprechenden Diensten stehen. Unter Umständen sind diese Nutzungsmodelle vor der Verbreitung entsprechender Dienste nachzuweisen, so dass also ein verschärftes Zulassungsverfahren für entsprechende Dienste denkbar wäre. In jedem Fall müssen die Betreiber zu deutlich stärkerer Transparenz gezwungen werden. Des Weiteren müssen die Betreiber territoriale Daten wie durch ein Schengen Routing herstellbar akzeptieren.

Außerdem sollten die Betreiber dazu angehalten werden, ihre AGBs klarer und einfacher zu formulieren.

7. Welchen Beitrag können Vorschläge wie DE-Mail oder Schengen-Routing tatsächlich leisten und müsste nicht die zentrale Maßnahme sein, schnell vertrauenswürdige und wirksame Ende-zu-Ende-Verschlüsselung durchzusetzen? Welche Maßnahmen müssen ergriffen werden, um hierfür die jeweiligen Systemumgebungen abzusichern und zugleich die Handhabbarkeit zu erleichtern? Inwieweit sollten Telekommunikationsanbieter zu einer Transportverschlüsselung verpflichtet werden?

Zu den Fragen wurde oben bereits Stellung genommen. All diese Maßnahmen sind hilfreich, wobei insbesondere Schengen-Routing und Verschlüsselung eine andere und bessere Ausgangslage gegen kommerzielle und nachrichtendienstliche Massenüberwachung herstellen. Gegen gezielte Überwachung und Spionage sowie Industriespionage sind die Maßnahmen isoliert ungeeignet. Hierzu müsste die eingangs erwähnte umfassende Reform der gesamten IT-Umgebung stattfinden. Eine Systemumgebung mit einem „weak link“ ist für starke Angreifer über diesen schwachen Link meist vollständig kompromittierbar. Eine Verpflichtung zu einer Transportverschlüsselung macht von daher als Maßnahme gegen Massenüberwachung Sinn, allerdings nicht gegen Spionage.

8. Wo sehen Sie gesetzgeberischen Handlungsbedarf, um den Grundrechtsschutz und den Schutz der Vertraulichkeit der Kommunikation sicherzustellen?

Entsprechende Vorschläge wurde im Laufe des Textes bereits gemacht.

9. Welchen Beitrag kann das Bundesamt für die Sicherheit in der Informationstechnik (BSI) zur Erhöhung der IT-Sicherheit und zur Unterstützung des Selbstschutzes der Bürgerinnen und Bürger sowie der Unternehmen leisten, welche Rahmenbedingungen müssen hierfür erweitert und welche personellen sowie materiellen Grundlagen geschaffen werden? Inwieweit müssen welche Kapazitäten des BSI und auch des Cyber-Abwehrzentrums ausgebaut werden? Wie kann das BSI in seiner Rolle als neutraler Berater der Bürgerinnen und Bürger gestärkt werden? Inwieweit ist eine effektive Koordinierung mit dem BMI und den anderen Ressorts der Bundesregierung gesichert?

Das BSI ist eine wichtige und zentrale Institution für die IT-Sicherheit in Deutschland und muss dringend verstärkt werden. Die Behörde leistet gute und wichtige Arbeit für den Grundschutz der Bürgerinnen und Bürger, muss jedoch stärker angehalten werden, auch andere und neuere Themen effektiv anzugehen und die Industrie besser zu schützen. So sind etwa Hochsicherheit und die Verwundbarkeiten von Basistechnologien zu adressieren, Probleme der Industriespionage und der Schutz kritischer Infrastrukturen vor Angreifer in der Qualität der NSA. Hierfür muss das BSI personell besser ausgestattet werden, mit der Möglichkeit der Zahlung flexibler und industriefähiger Gehälter, um bessere Expertise in der Breite zu erreichen. Außerdem wäre es wünschenswert, wenn das BSI mit höheren Kompetenzen und Eingriffstiefen ausgestattet werden würde, um in kritischen Kontexten stärker regulieren zu können. Die Koordinierung durch das BMI ist effektiv, zu anderen Ressorts bestehen dagegen nur sporadische Kontakte und durch Interessenskonflikte der Ressorts Handlungshemmungen.

10. Wie können angemessene IT-Sicherheitsaudits für Open Source Security Software ermöglicht werden und wie können das BSI oder andere, auch nicht-staatliche Stellen, derartige Audits unterstützen?

Entsprechende Audits müssen vorrangig durch eigens abgestelltes, ausreichend befähigtes Personal durchgeführt werden. Eine Verwendung von automatisierten Prüfverfahren ist nur begrenzt sinnvoll und dürfte in diesem Fall wenig Gewinn bringen. Da dieses Personal sehr gut geschult und fähig sein muss und da das Prüfen von Code eine langweilige und anstrengende Aufgabe ist, ist dies vor allem eine Frage monetärer Ressourcen. Hier könnten internationale Partnerschaften angestrebt werden, um die Kosten zu teilen. Nicht-staatliche Stellen kommen aufgrund möglicher Interessenskonflikte eher nicht in Frage und müssten in jedem Fall zuvor überprüft werden. Zudem ist sicherzustellen, dass keine Nachrichtendienste oder Kriminelle die Audits unterminieren. Dennoch bleibt ein hohes Restrisiko, wie eingangs dargestellt wurde. Die Überprüfung von Code ist nur begrenzt möglich, nur begrenzt effizient, beseitigt bei weitem nicht alle Sicherheitsprobleme und kann durch andere unsichere Elemente der gleichen Umgebung wieder kompromittiert werden.

11. Sehen Sie die Vorschläge der EU-Datenschutzgrundverordnung als ausreichend an, um ausländischen Unternehmen (Facebook, Google, WhatsApp etc.), die in Europa ihre Dienste anbieten, zur Wahrung der europäischen Datenschutzgrundsätze zu verpflichten oder wo besteht aus Ihrer Sicht noch Handlungsbedarf? Welche Möglichkeiten bestehen, europäische Bürgerinnen und Bürger bei der Nutzung entsprechender Angebote vor dem Ausspähen durch ausländische Dienste zu schützen? Wie schätzen Sie weitere EU-Legislative (z.B. die Cybercrime-Richtlinie) diesbezüglich ein?

Die Vorschläge sollten um Forderungen zu hoher Transparenz der Unternehmen im Bezug auf deren geschäftliche Nutzung der durch sie erhobenen Daten ergänzt werden. Ohne Kenntnis der genauen Nutzungsformen, auch der Speicherung, der Anonymisierung, der Territorialitäten der Daten etc. sind vom Bürgern unter Umständen keine vollumfänglich informierten Entscheidungen zu machen. Zwar lassen sich auch auf reduzierter Faktenbasis informierte Entscheidungen treffen (etwa allein aufgrund der realen Konsequenzen), eine umfassendere Information sowie eine begleitende mediale und politische Aufklärung sind prinzipiell wünschenswert, um die Entscheidungsfindung zu verbessern. Davon abgesehen müssen die Verordnungen in ihrer Implementierung begleitet werden, um keine Schlupflöcher für die IT-Unternehmen zu bieten. Hierzu bestehen bereits sehr starke Lobby-Aktivitäten in Brüssel und Berlin. Technisch nicht ausreichend versierte Gesetzgeber können dabei leicht in trügerische Formulierungen und Vorschläge geführt werden. Des Weiteren ist sicherzustellen, dass Verstöße bemerkt werden und dass Strafen in einer Höhe erfolgen, die eine ausreichend Abschreckungswirkung für die Unternehmen erzielt.

Der Schutz vor einer Ausspähung durch ausländische Dienste über ausländische IT-Unternehmen ist vor allem durch eine Forcierung der Territorialität der Daten durch Schengen-Routing und Schengen-Datenhaltung zu gewährleisten und durch eine effiziente, kontrollierbare und strafbare Regulierung dieser territorialen Daten. Sobald die Daten den europäischen Raum verlassen, bestehen keinerlei Ansprüche jenseits der in den AGB der Unternehmen zugesicherten Kriterien, wobei auch diese durch geheim rechtliche Verpflichtungen unterminiert sein können. Territorialität ist folglich eine condicio sine qua non. Verstöße gegen diese wichtige Vorbedingungen sollten unter Umständen den Ausschluss vom europäischen Markt nach sich ziehen.

Dr. Sandro Gaycken
FU Berlin
Mai 2014, Berlin