Auf dem Weg zur unsicheren und gläsernen digitalen Welt

Alles wissen, alles entschlüsseln, auf alles zugreifen

Die Veröffentlichung des NSA-Skandals jährt sich zum zweiten Mal, doch wie groß ist das Interesse an weiteren Aufklärungen? Welche Lehren wurden aus dem Fundus der Snowden-Dokumente gezogen und wie düster sieht die Zukunft der Datensicherheit insbesondere hinsichtlich politischer Signale, zum Beispiel zur Schwächung von Verschlüsselungen, aus? Und: Wie ist der Stand der Dinge rund um den NSA-Skandal in Deutschland? Folgender Beitrag zieht eine Zwischenbilanz.*)

Die Vertrauenswürdigkeit, auch unter international fest verankerten Partnern, ist aus der Sichtweise der Öffentlichkeit stark angeschlagen – könnte man meinen. Immerhin wurde ein Diensthandy unserer Kanzlerin abhört. Was folgte, war ein diplomatisches Gezanke, ob dies der Wahrheit entspricht und ob weiter hochrangige Staatsbedienstete abgehört werden. Fakt ist leider, dass jeden Tag sehr großzügig die persönlichen Daten von allen Bundesbürgern durch Geheimdienste mitgelesen und ausgewertet werden. Die Regierung unter der Leitung von Angela Merkel sieht nur tatenlos zu, wie jeden Tag die Privatsphäre der Bundesbürger verletzt wird und der Schutz der Werte der Bundesbürger nicht angemessen erbracht wird.

Dem nicht genug, folgte im Mai 2014 der Krimi um den vermeidlichen Spion Marcus R., der beim Bundesnachrichtendienst (BND) unter anderem brisante Dokumente über die Ziele der Auslandsaufklärung vermutlich an die Central Intelligence Agency (CIA) weitergegeben hat. Die Bundesregierung, die mit ihren Anfragen über die geheimdienstlichen Aktivitäten in den USA stets mit politischen Floskeln abgespeist wurde, reagierte mit der Ausweisung des obersten Berliner CIA-Chefs, der das Land in Richtung Heimat verlassen musste. Das Auswärtige Amt, es hatte fast einen verzweifelten Unterton, hat daraufhin die US-Regierung zur Benennung aller Agenten in Deutschland aufgefordert (Matthias Gebauer und Jörg Schindler 2014). Dies geschah wohl aus dem Grund, um nicht den Eindruck zu erwecken, tatenlos dazu stehen, und um ein weiteres klares Zeichen auf dem diplomatischen Weg in Richtung Washington zu senden.

Wurde beim BND bisher in Richtung USA ein Auge zugedrückt, so soll nun auch in Richtung Westen geschaut werden, heißt es aus Regierungskreisen (Tagesschau.de 2014). Was die Bundesregierung bis dato verschwieg, ist, dass der BND und die National Security Agency (NSA) bereits seit Jahren kooperieren und gemeinsam Daten auswerten. Diese Information wurde im Oktober 2014 durch ein Rechercheteam bestehend aus Süddeutscher Zeitung, WDR und NDR veröffentlicht (Georg Mascolo, Hans Leyendecker, John Goetz 2014) und wird aktuell in Medien diskutiert.

Langjährige Kooperation zwischen BND und NSA

Zwischen 2004 und 2008 sollen demnach an Knotenpunkten in Frankfurt durch den BND im großen Stil Daten mitgelesen und, zusammen mit der NSA, ausgewertet wor-

den sein. Selbst Mitarbeitern des BND war diese Aktion hinsichtlich der Rechtmäßigkeit nicht geheuer, weil die Prüfung der Daten auf das Vorhandensein von sensiblen Inhalten auch von deutschen Bürgern, insbesondere bei verschlüsselten Datenpaketen, nicht ausreichend gesichert war (Kai Biermann 2014). Das Weiterleiten von Daten an ausländische Geheimdienste ist zwar zulässig, aber nur unter strengen Kontrollen. Aus den veröffentlichen Dokumenten geht hervor, dass die Mitglieder der G-10-Kommission möglicherweise genau hinsichtlich dieser strengen Kontrollen getäuscht wurden. Die G-10-Kommission besteht im Übrigen aus vier Mitgliedern und jeweils vier Vertretern, wobei der Vorsitzende die Befähigung zum Richteramt besitzen muss. Der BND hatte zwar eine Filtertechnik mit dem Namen „Dafis" installiert, die dafür sorgen sollte, dass Daten deutscher Bürger nicht weitergeleitet werden, der Filter funktionierte aber nicht zuverlässig. Es muss also davon ausgegangen werden, dass jahrelang personenbezogene Daten von deutschen Bürgern an die NSA weitergeleitet und ausgewertet wurden. Das Kanzleramt wusste schon 2008 von der NSA-Spionage (Zeit-Online 26.04.15).

Wir müssen auch zukünftig davon ausgehen, dass die NSA weiter an ihrem Potenzial für eine weltweite Datensammlung arbeitet, ob mit oder ohne die Zusammenarbeit der Geheimdienste in den betroffenen Ländern. Dies belegen die Aussagen des neuen NSA-Chefs Michael Rogers, der sich auch für einen Zugriff auf alle Verschlüsselungsschlüssel aussprach. Da sich zu Recht die Technologiebranche geschlossen gegen diesen Wunsch aussprach, wird der Geheimdienst wohl auch weiterhin daran arbeiten, sich unbemerkt Zugriff auf verschlüsselte Informationen, insbesondere in stark abgesicherten Infrastrukturen, zu verschaffen.

Warum wir die IT-Sicherheit ausländischer Dienste und Produkte neu bewerten müssen

Wir haben aus dem NSA-Skandal gelernt, dass auf die Sicherheit von Hardware- und Softwarekomponenten auch von befreundeten Nationen nicht mehr ohne weitere Prüfungen vertraut werden kann. Am Beispiel der Vereinigten Staaten von Amerika lässt sich festhalten, dass Gesetzgebungen wie beispielsweise der Patriot Act den Geheimdiensten nahezu jeglichen Zugriff auf die durch US-Hersteller und -Unternehmen erfassten Daten gewähren, selbst wenn diese Daten außerhalb der USA erhoben wurden. Ein Beispiel dafür sind Daten, die in Cloud-Computing-Services in Europa gespeichert werden. Am 1. Juni steht der US Congress vor einer neuen Abstimmung, ob der selbst in den USA mittlerweile umstrittene Patriot Act verlängert wird oder nicht (Trevor Timm 2015).

Als ob der staatlich verordnete Datenhunger nicht schon groß genug ist, werden US-Geheimdienste auch selber tätig und bauen nachträglich Hintertüren (Backdoors) zum Beispiel in Router ein, um diese überwachen zu können. Dies geht aus Dokumenten von Edward Snowden hervor, und verantwortlich für diese kleinen Extra-Features sind die Spezialisten der Tailored Access Operations (TAO) (Martin Holland 2014a). Diese Einheit ist der NSA unterstellt und sorgt dafür, dass Zugriffe auch auf gut gesicherte Netzwerke erlangt werden. Da die TAO eine der besten Cybereinheiten der US-Geheimdienste ist, würde es kaum verwundern, wenn herauskäme, dass Spezialisten dieser Truppe Mitentwickler des Computerwurms Stuxnet waren. Stuxnet hat in den Jahren 2009 und 2010 unter anderem Zentrifugen zur Urananreicherung der iranischen Atomanlagen in Natanz befallen und für das politische Ziel der Amerikaner und Israelis gesorgt, dass das dortige Atomprogramm um mehrere Jahre zurückgeworfen wurde. Auch die Spionagesoftware Regin wird dem US-Nachrichtendienst NSA und dem britischen Geheimdienst GCHQ zugesprochen. Diese Art von Trojaner war unter anderem auf einem privaten Computer einer Mitarbeiterin im Bundeskanzleramt entdeckt worden (Martin Holland 2014b). Die These für eine Verbindung zu den westlichen Nachrichtendiensten wird dadurch gestützt, dass die Schadsoftware ähnlich komplex ist wie Stuxnet und dass dies laut verschiedenen IT-Sicherheitsexperten das Werk von staatlichen Organisationen sein kann.

Vertrauensverlust in ausländische Dienste führt zum Umdenken

Dass die Bundesregierung ein hohes Maß an Vertrauen in US-Unternehmen gelegt hat, konnte im letzten Jahr noch jeder Internet-Nutzer über eine einfache IP-Adress-Abfrage nachvollziehen. Demnach waren noch im Juni 2014 die Mitarbeiter und Abgeordneten im Bundestag über den US-amerikanischen Telekommunikationsanbieter Verizon mit dem Internet verbunden (Andre Meister 2014). Um keine weiteren Risiken einzugehen, hat das Bundesministerium des Innern bereits reagiert und mit folgendem Statement darauf hingewiesen, dass die Infrastruktur von Verizon zukünftig nicht mehr genutzt wird: „Die heutige Regierungskommunikation stützt sich im Wesentlichen auf die beiden Netzinfrastrukturen IVBB (Informationsverbund Berlin-Bonn)

) Der Beitrag wurde kurz vor den aktuellen Enthüllungen im Zusammenhang mit NSA/BND verfasst. Die Redaktion hat die Autoren gebeten, bei Gelegenheit auch hierzu eine Einschätzung zu geben. Diese werden zu gegebener Zeit auf unserem Online-Portal unter www.datakontext.com/bnd veröffentlicht.

und IVBV/BVN (Informationsverbund der Bundesverwaltung/Bundesverwaltungsnetz) sowie das Bund-Länder-Verbindungsnetz (Deutschland-Online-Infrastruktur – DOI). Die Netzdienstleistung für den für die Kommunikation der Ministerien verwendeten IVBB wird durch die Telekom bereitgestellt." Des Weiteren haben „[…] die im Zuge der NSA-Affäre aufgezeigten Beziehungen von fremden Nachrichtendiensten und Firmen gezeigt, dass für die sicherheitskritische Kommunikationsinfrastruktur der Bundesregierung besonders hohe Anforderungen zu stellen sind". (Bund 2014). Diese Reaktion zeigt immerhin, dass die Bundesregierung bereit ist, eine von vielen Baustellen zur Steigerung der IT-Sicherheit in Deutschland anzugehen. Ein großes Negativbeispiel in Berlin zeigt nach einer Anfrage der Piratenpartei mit dem Stand 31.09.2014, dass in der Finanzverwaltung, in der Justizbehörde und in der Senatskanzlei immer noch Computer (insg. 28.477) mit dem 13 Jahre alten und nicht mehr als sicher eingestuften Betriebssystem Windows XP von Microsoft ausgestattet sind.

Wie stehen andere Staaten zum Thema IT-Sicherheit?

Wie es auch anders in puncto IT-Sicherheit laufen kann, zeigt ein Beispiel bei der Kooperation zwischen der russischen Regierung und Microsoft. Demnach legte der US-Konzern bereits seit 2003 seinen Quellcode oder zumindestens Teile davon offen, damit Russland diesen prüfen kann (Eric Auchard, David Clarke 2014).
China ist hier noch weitaus konsequenter vorgegangen und hat die Nutzung von einigen ausländischen Produkten im öffentlichen Dienst komplett verboten. Es war nicht mehr erlaubt, mit öffentlichen Geldern beispielsweise Apple-Produkte anzuschaffen (Richard Meusers 2014; Leo Becker 2014). Auch die sehr deutlichen Worte des Staatssenders CCTV, die vor der Ausweitung dieses Verbots bereits über das iPhone berichteten und es als „[…]Gefahr für die nationale Sicherheit […]" bezeichneten (Paul Carsten 2014), trugen zu erschwerten Wirtschaftsbedingungen bei. Das iPhone könne dafür benutzt werden, Staatsgeheimnisse auszuforschen und um die ökonomische Situation im Land zu analysieren, wurde berichtet. Diese Aussage war Teil einer breiteren Medienkampagne, welche die Servicequalität und Gefahren durch Nutzertracking des iPhones sehr kritisch darstellten. Mittlerweile ist China für Apple zu einem der umsatzstärksten Märkte weltweit aufgestiegen. Ob dies unter anderem mit den durch Tim Cook (Apple CEO) am Anfang des Jahres öffentlich zugesicherten Code-Reviews (Grant Gross 2015) der Betriebssystem-Quellen zu tun hat, bleibt offen.

China selbst hingegen steht ebenso wie die USA, Russland, Großbritannien, … „unter dem Verdacht" staatliche Hacker zu beschäftigen. Im März 2015 wurde dies sogar durch ein offizielles Dokument einer staatlichen Organisation bestätigt (Shane Harris 2015). Auch in dem jährlich erscheinenden Report des amerikanischen Verteidigungsministeriums werden die chinesischen Kapazitäten der elektronischen Kriegsführung als sehr fortschrittlich bezeichnet (Department of Defence – USA 2014). Der chinesische Staatschef Xi Jinping, Vorsitzender der

zentralen Führungsgruppe für Internetsicherheit und Informationspolitik, äußerte sich sinngemäß mit den Worten: „Es müssen Anstrengungen vorangetrieben werden, um das Land in eine Cyber-Macht zu verwandeln" (Zhu Ningzhu 2015). Russische Hacker sollen sich Zugang zu E-Mail-Archiven des Weißen Hauses verschafft haben (siehe Heise News vom 26.04.15). Die Großmächte rüsten im Cyberspace auf und machen dadurch das Internet zum neuen Schlachtfeld, was sicher schwerwiegende negative Konsequenzen für den weiteren Erfolg des Internets haben wird.

Politiker sprechen sich für Hintertüren in Verschlüsselungen aus

Eine große aktuelle Gefahr für die IT-Sicherheit und den Datenschutz im Internet könnte der Wunsch verschiedener Politiker hinsichtlich einer Schwächung beziehungsweise eines Einbaus von Hintertüren in Verschlüsselungen werden. Politiker wie der US-Präsident Barack Obama und der britische Premierminister David Cameron sprachen sich kürzlich für Hintertüren in Verschlüsselungen aus. David Cameron wollte dafür sogar einen neuen Begriff prägen, die sogenannte „front door", zu Deutsch Vordertür, die gesetzlich verankert und ganz legal Verschlüsslungen umgehen kann (Julian Hattem 2015). Auch der deutsche Innenminister Thomas de Maizière äußerte sich zu diesem Themenkomplex. Deutsche Sicherheitsbehörden müssten „befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen" (Markus Böhm 2015), sagte de Maizière. Dabei wurde noch im Leitdokument zur „digitalen Agenda" eine bessere Verschlüsselung angestrebt: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 auf der Welt werden", so der Originaltext, an dem auch das Bundesministerium des Innern mitgewirkt hat. Hier wird das Problem deutlich, dass das Bundesinnenministerium sowohl für die Strafverfolgung als auch für die IT-Sicherheit verantwortlich ist. Das Problem ist aber, dass im Prinzip beide Punkte nicht miteinander zu vereinbaren sind.

Schon heute haben Strafverfolgungsbehörden die Möglichkeit, mittels Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) auf Informationen zuzugreifen, die auf Computern oder Smartphones potenzieller Straftäter oder sogenannter Gefährder liegen. Dabei können Konversationen schon in den Geräten abgefangen werden, bevor sie für die Kommunikation verschlüsselt werden. Zu Recht werden diesen Maßnahmen enge Grenzen gesetzt. Sie dürfen nur mit richterlichen Anordnungen eingesetzt werden. Weiterhin ist auch diese Methode sehr umstritten, denn die Quellen-TKÜ ist ein gravierender Eingriff in die Grundrechte eines Betroffenen. Maßnahmen zur Schwächung der Verschlüsselung könnten wiederum eingesetzt werden, um in Massenüberwachung auch unbescholtene Bürger zu überwachen. Dies darf so nicht durch- und umgesetzt werden.

Wirtschaftliche Folgen durch Geheimdienstaffären

Auch dass die Implementierung von Schnittstellen zum Ausliefern von Daten mit Millionenunterstützungen durch Geheimdienste gefördert wird, wirft ein verstörendes Licht auf den geheimdienstlichen Machtapparat in den USA.

Unter diesem Gesichtspunkt wird besonders die Unwirksamkeit des Safe-Harbor-Abkommens zum Schutz von im europäischen Wirtschaftsraum (EWR) erhobenen Daten, welche in die USA übermittelt werden, deutlich. Eine Überarbeitung dieser Richtlinie zum Schutz von Millionen EU-Bürgern ist deshalb von hoher Wichtigkeit. Wird eine Beendigung von Safe Harbor durchgesetzt, wird dies auch dazu führen, dass eine Weiterentwicklung der Europäischen Datenschutzvereinbarung vorangetrieben werden muss und nicht, wie momentan üblich, hinausgezögert wird. Ziel sollte es sein, unmittelbar einen hohen Datenschutz für die Bürger und Unternehmen der Europäischen Union zu erwirken und nicht große Firmen mit einem Hauptsitz außerhalb der EU durch eine Blockade bei der Erstellung geeigneter Richtlinien vorerst weiter zu schützen. Die Richtlinien müssen hohe Strafen für Verstöße enthalten. Die Nachweisbarkeit von Datenschutzverstößen ist jedoch eine komplexe Angelegenheit und kann wohl nur aufgedeckt werden, wenn Whistleblower wie beispielsweise Edward Snowden zum Gegenschlag auf umfassende Geheimdienstprogramme ausholen.

Wirtschafts- und Rüstungsspionage

Vor der Aufdeckung der Abhörprogramme der NSA durch Edvard Snowden wussten viele Experten bereits, dass Gruppierungen auf illegale Methoden zum Abgreifen von geheimen Informationen in den Bereichen Rüstung und Wirtschaft zurückgriffen. Es ist auch bekannt, dass unverschlüsselte Kommunikation von Geheimdiensten an zentralen Knotenpunkten abgefangen und ausgewertet wird. Dabei kommen nicht selten fortschrittliche Trojaner zum Einsatz. Täter sind Staaten, kriminelle Organisationen oder Einzeltäter, die aus gesammelten Daten wichtige Erkenntnisse erbeuten und diese dann zum Vorteil für sich verwenden wollen. Staaten nutzen diese Methode zur Verfolgung von international agierenden Kriminellen oder Terroristen. Verwunderlich ist es nicht, dass auch Rüstungsunternehmen wie beispielsweise Lockheed Martin Mitte 2011 zum Ziel von Hackern wurden (Markus Ströbe 2011). Der Angriff auf Lockheed Martin wurde durch die zuvor bei RSA erbeuteten Informationen über den RSA-Token (Daniel Bachfeld 2011) langfristig und hoch professionell vorbereitet. Im April 2009 kam es zuvor schon zu einem Hackerangriff auf Informationen über den Tarnkappenjet F35 im US-Verteidigungsministerium. Dies könnte erklären, warum der von China entwickelte Tarnkappenjet J-20, der im Januar 2011 präsentiert wurde, eine sehr große Ähnlichkeit zum Kampfjet der Amerikaner aufweist und zudem noch die neueste Tarnkappentechnik besitzt (mbe 2012), aber natürlich sind dies reine Spekulationen.

Ein sehr gut dokumentierter Fall von Spionage ereignete sich zum Beispiel im Jahr 1996 (Ludwig Rademacher 1996). Damals war der Windkrafthersteller Enercon wohl Opfer von gezielter Spionage. Es wurde zukunftsweisende und sehr effektive Technologie für die Stromerzeugung durch Windkraft kopiert. Ein Unternehmen in den USA ließ sich letztendlich die wertvollen Technologien patentieren und verklagte sogar das deutsche Unternehmen.

Im Rahmen der NSA-Abhörmaßnahmen rücken auch solche Vorkommnisse wieder in einen aktuellen Fokus. Auch die gezielte Schwächung von Crypto-Algorithmen können die US-Geheimdienste nutzen, um nicht nur auf den verschlüsselten Kanälen von Privatpersonen mitzulesen. Auch die Kommunikation von Industrie- und Wirtschaftsgeheimnissen kann auf diese Weise abgefangen werden. Leider können das die kriminellen Organisationen, Terroristen und sonstige Angreifer auch, wenn die Art der Schwächung bekannt ist. Die Schwächung von Crypto-Algorithmen, IT-Sicherheitssystem und IT-Systeme sorgt zwar für einen „einfachen" Zugriff der Geheimdienste auf die gewünschten Daten, aber die IT-Sicherheit des Internets wird kompromittiert und unsere Werte angreifbar!

Schäden durch Wirtschaftsspionage

Der Bundesinnenminister a.D. Hans-Peter Friedrich ging 2013 davon aus, dass der Schaden durch Wirtschaftsspionage alleine in Deutschland bei einem Volumen von ca. 50 Milliarden Euro liegt. Eine aktuelle Studie ergibt, dass mittlerweile jedes zweite Unternehmen bereits von Datendiebstahl und Wirtschaftsspionage betroffen ist. Dies ergab eine Umfrage des BITKOM unter Führungskräften und Sicherheitsexperten bei Unternehmen mit mehr als zehn Mitarbeitern. Der geschätzte Schaden von 51 Milliarden deckt sich dabei fast mit den Thesen von Hans-Peter Friedrich, es wird sogar von einem Anstieg um eine Milliarde Euro ausgegangen.

Zwischen staatlicher Spionage und kriminellen Hackerangriffen kann dabei kaum eindeutig unterschieden werden. Durch die NSA-Affäre ist klar geworden, dass Geheimdienste wie die NSA die gleichen Methoden wie kriminelle Hacker nutzen. Dabei infiziert die NSA weltweit bis zu 100.000 Computer mit Schadsoftware (Nico Ernst 2014), auf denen dann sehr einfach geheime Informationen abgefangen werden können.

Warum aber ist es so schwierig, beispielsweise im Fall Stuxnet oder Regin genau zu ermitteln, wer für Angriffe verantwortlich ist? Schließlich gibt es bei jedem Angriff eine IP-Adresse und dazu einen Besitzer. Aber ist der Besitzer der IP-Adresse auch der Täter des Angriffs? Dies bleibt häufig im Dunkeln, weil viele infizierte Computer weltweit als Zwischenstation für Angriffe verwendet werden. Angreifer nutzen dazu so genannte „Hops", also Stationen, auf denen sie eine Schadsoftware platziert haben, um sie für ihre anonymisierten Angriffe ausnutzen zu können. Demnach kann beispielsweise ein Angreifer aus Deutschland über mehrere Zwischenstationen, möglicherweise in Russland, dann in China, einen Angriff so aussehen lassen, als ob er aus China ausgeführt wurde. Dieses Beispiel zeigt sehr anschaulich, wie einfach es für Hacker oder Geheimdienste sein kann, ihre Angriffe zu vertuschen.

IT-Sicherheit rückt immer mehr in den Fokus

Ziel sollte sein, das Verständnis für IT-Sicherheit, den Datenschutz und ein Recht auf Verschlüsselung weiter zu sichern und durchzusetzen. Dies kann gefördert werden, indem gezielt auf die Internet-Nutzer aller Altersklassen eingegangen wird. Mittelständische und kleine Unternehmen sollten gezielt durch weitere Task-Force-Förderungsmaßnahmen unterstützt werden. Das Institut für Internet-Sicherheit hat zum Beispiel bereits mit dem Projekt IT-Sicherheit im Handwerk IT-Sicherheitsbotschafter ausgebildet. Auch mit jungen Menschen wurde mit der Cyber Security Challenge Germany ein Projekt gestartet, um IT-Sicherheitstalente zu identifizieren und zu fördern (www.CSCG.de). Diese Maßnahmen können auch dem allzu oft gehörten Satz „Was wollen Geheimdienste mit meinen Daten, ich habe doch sowieso nichts zu verbergen" entgegenwirken. Ein besseres Verständnis rund um das Thema IT-Sicherheit führt aber

auch dazu, dass private sowie wirtschaftliche Schäden durch mangelndes Wissen über Risiken bei der Nutzung von IT-Systemen, also auch sozialen Medien, mobilen Apps und der allgemeinen Nutzung von Smart-Devices, reduziert werden können.

Wenig Erfolge durch Massenüberwachungen in den USA

In welchem Umfang die massiven und sehr teuren Überwachungen durch die Geheimdienste Wirkung zeigen, ist kaum zu beziffern. In den USA wurde eine Studie im Auftrag der New America Foundation veröffentlicht (Cahall 2014), welche die möglichen Erfolge der Massenüberwachung durch US-Geheimdienste in Frage stellt. Demnach wurden die Informationsquellen untersucht, die zur Verhaftung von 225 Personen geführt haben. Ziel der Personen war die Planung von Attentaten und Anschlägen auf Einrichtungen in den USA. Aufgrund der Verhaftung dieser Personen wurden der Studie zufolge 50 Attentate verhindert. Die Summe dieser Attentate wurde auch aus dem Statement vom ehemaligen NSA-Chef Keith Alexander vor dem US Congress entnommen. Informationen zur Festnahme der Terrorverdächtigen stammten überwiegend von Familienmitgliedern oder Bekannten (17,8 Prozent), sowie von Informanten, die keinem genaueren Umfeld zugeordnet werden konnten (16 Prozent). Die durch die NSA betriebenen Überwachungsprogramme im Ausland konnten gerade einmal 7,5 Prozent der Fälle aufdecken; beim Telefonüberwachungssystem im Inland waren es 1,8 Prozent. In genau einem Fall konnte durch die Telefonüberwachung eine Person in den USA identifiziert werden. Diese Person hatte Verbindungen zu einer Terrormiliz und hat 8.500 US-Dollar nach Somalia über-

Literaturverzeichnis

- ***Andre Meister (2014):*** *Arbeitserleichterung für die NSA: Deutscher Bundestag bezieht Internet von US-Anbieter Verizon. Hg. v. Netzpolitik.org. Online verfügbar unter https://netzpolitik.org/2014/arbeitserleichterung-fuer-die-nsa-deutscher-bundestag-bezieht-internet-von-us-anbieter-verizon/, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Bund (2014):*** *Bund wechselt Netzbetreiber. Hg. v. Bundesministerium des Innern. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/06/bund-wechselt-netzbetreiber.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Cahall, Bailey (2014):*** *Do NSA's Bulk Surveillance Programs Stop Terrorists? Hg. v. New America Foundation, zuletzt geprüft am 16.04.2015.*
- ***Daniel Bachfeld (2011):*** *RSA-Hack könnte Sicherheit von SecurID-Tokens gefährden. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/security/meldung/RSA-Hack-koennte-Sicherheit-von-SecurID-Tokens-gefaehrden-1210245.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Department of Defence – USA (Hg.) (2014):*** *ANNUAL REPORT TO CONGRESS. Military and Security Developments Involving the People's Republic of China 2014. Online verfügbar unter http://www.defense.gov/pubs/2014_DoD_China_Report.pdf.*
- ***Eric Auchard, David Clarke (2014):*** *Russia wants Apple, SAP to cooperate against foreign spying. Hg. v. Reuters.com. Online verfügbar unter http://uk.reuters.com/article/2014/07/30/russia-software-idUKL6N0Q52UD20140730, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Friedhelm Greis (2014):*** *Studie sieht wenig Erfolge durch Massenüberwachung. Hg. v. Golem.de. Online verfügbar unter http://www.golem.de/news/nsa-affaere-studie-sieht-wenig-erfolge-durch-massenueberwachung-1401-103896.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Georg Mascolo, Hans Leyendecker, John Goetz (2014):*** *Codewort Eikonal – der Albtraum der Bundesregierung. Hg. v. Süddeutsche Zeitung. Online verfügbar unter http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432.*
- ***Grant Gross (2015):*** *Report: Apple agrees to Chinese security audits of its products. Hg. v. itworld.com. Online verfügbar unter http://www.itworld.com/article/2874235/report-apple-agrees-to-chinese-security-audits-of-its-products.html, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*
- ***Julian Hattem (2015):*** *Obama backs call for tech backdoors. Hg. v. thehill.com. Online verfügbar unter http://thehill.com/policy/technology/229787-obama-backs-call-for-tech-backdoors, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*
- ***Kai Biermann (2014):*** *BND schickte wissentlich Daten von Deutschen an die NSA. Hg. v. Zeit.de. Online verfügbar unter http://www.zeit.de/digital/datenschutz/2014-10/bnd-nsa-de-cix-daten-eikonal, zuletzt aktualisiert am 13.04.2015, zuletzt geprüft am 13.04.2015.*
- ***Leo Becker (2014):*** *China: iPhone ist Bedrohung für die nationale Sicherheit. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/mac-and-i/meldung/China-iPhone-ist-Bedrohung-fuer-die-nationale-Sicherheit-2257924.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Ludwig Rademacher (1996):*** *ENERCON: Spione im Wind. Hg. v. Focus.de. Online verfügbar unter https://www.focus.de/finanzen/news/enercon-spione-im-wind_aid_162267.html.*
- ***Markus Böhm (2015):*** *Thomas de Maizière: Innenminister sieht Verschlüsselung als Problem. Hg. v. Spiegel.de. Online verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/thomas-de-maiziere-innenminister-wendet-sich-gegen-verschluesselung-a-1014244.html, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*
- ***Markus Ströbe (2011):*** *Hacker steigen bei Lockheed Martin ein. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/security/meldung/Hacker-steigen-bei-Lockheed-Martin-ein-1251902.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- ***Martin Holland (2014a):*** *NSA manipuliert per Post versandte US-Netzwerktechnik. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html?hg=1&hgi=2&hgf=false, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*

wiesen. Dieses Beispiel zeigt sehr deutlich, wie uneffektiv ein solches Überwachungssystem wirklich ist.

Fazit

Die NSA fügt in IT-Sicherheitsprodukte Hintertüren ein, manipuliert IT-Sicherheits-Standards und -Technologien und macht daher unser Geschäftsleben und unsere Internet-Aktivitäten unsicher. Schlechte Zufallszahlen in IT-Sicherheitsprodukten machen zum Beispiel die Verschlüsselung nutzlos! Wir zahlen viel Geld für Verschlüsselungsprodukte, die keinen Nutzen für uns haben. Nicht nur die NSA nutzt diese Schwachstelle, um Zugriff auf unsere Daten zu haben, sondern auch kriminelle Organisationen und Wirtschaftsspione. Die NSA gibt jährlich 70 Milliarden Dollar für Spionage aus, und einen großen Teil davon verwendet sie dafür, die IT-Sicherheit des Internet zu kompromittieren und unsere Werte angreifbar zu machen!

Aus diesem Grund ist jeder Staat gezwungen, eigene vertrauenswürdige IT-Sicherheitslösungen zu etablieren, um Spionage und Hacking-Angriffen durch Cyberkriminelle vorzubeugen. Deutschland kann nicht mehr blind und ohne Kontrollen auf die IT-Sicherheit von Technologien aus dem Ausland vertrauen. Da sind leider auch westliche Staaten wie die USA und Großbritannien inbegriffen, die, durch die Snowden-Dokumente belegte, rigorose Abhörpraktiken betreiben.

Alle Großmächte weltweit werden weiter an ihren Kapazitäten für eine defensiv und offensiv ausgelegte Cyberstrategie arbeiten. Die Dokumente aus dem Snowden-Fundus beschreiben lediglich den Stand der Fähigkeiten einer Großmacht bis zum Jahr 2013. Über heutige Methoden oder Programme, die eingesetzt werden, kann nur spekuliert werden. Sie werden aber immer fortschrittlicher, das steht fest. Fest steht auch, dass dadurch die Angreifbarkeit unserer Daten und IT-Systeme wächst. Die Lehren aus den Snowden-Dokumenten und dem NSA-Skandals sollten allen sehr klar sein! Die Bundesregierung, die deutsche Wirtschaft, die IT-Sicherheitsindustrie in Deutschland und die IT-Sicherheitsforschung müssen gemeinsame Ziele definieren und weiter an dem Thema IT-Sicherheit arbeiten, damit die Risikosituation in der Zukunft deutlich verbessert werden kann. ■

- *Martin Holland (2014b): Offenbar Spionagesoftware Regin auf Rechner im Kanzleramt entdeckt. Hg. v. Heise.de. Online verfügbar unter http://www.heise.de/security/meldung/Offenbar-Spionagesoftware-Regin-auf-Rechner-im-Kanzleramt-entdeckt-2507042.html, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*
- *Matthias Gebauer; Jörg Schindler (2014): Spionage: Regierung verlangt Aufdeckung aller Agenten in Deutschland. Hg. v. Spiegel.de. Online verfügbar unter http://www.spiegel.de/politik/deutschland/spionage-bundesregierung-aufdeckung-aller-agenten-in-deutschland-a-985199.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- *mbe (2012): Neues Modell: China enthüllt zweiten Tarnkappen-Kampfjet. Hg. v. Spiegel.de. Online verfügbar unter http://www.spiegel.de/wissenschaft/technik/china-enthuellt-tarnkappen-kampfjet-j-31-a-865031.html.*
- *Nico Ernst (2014): NSA-Software läuft auf 100.000 Computern. Hg. v. Heise.de. Online verfügbar unter http://www.golem.de/news/spaehaffaere-nsa-software-laeuft-auf-100-000-computern-1401-103912.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- *Paul Carsten (2014): Apple iPhone a danger to China national security – state media. Hg. v. Reuters.com. Online verfügbar unter http://in.reuters.com/article/2014/07/11/apple-china-iphone-idINKBN0FG0S820140711, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- *Richard Meusers (2014): China verbietet Apple-Computer im öffentlichen Dienst. Hg. v. Spiegel.de. Online verfügbar unter http://www.spiegel.de/netzwelt/web/china-verbietet-nutzung-von-apple-produkten-bei-behoerden-a-984878.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- *Shane Harris (2015): China Reveals Its Cyberwar Secrets. Hg. v. thedailybeast.com. Online verfügbar unter http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*
- *Tagesschau.de (Hg.) (2014): Der BND soll auch nach Westen schauen. Online verfügbar unter http://www.tagesschau.de/inland/bnd-gegenspionage-100.html, zuletzt aktualisiert am 14.08.2014, zuletzt geprüft am 14.08.2014.*
- *Trevor Timm (2015): Congress must end mass NSA surveillance with next Patriot Act vote. Hg. v. theguardian.com. Online verfügbar unter http://www.theguardian.com/commentisfree/2015/apr/08/congress-must-end-mass-nsa-surveillance-with-next-patriot-act-vote, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*
- *Zhu Ningzhu (2015): Xi Jinping leads Internet security group. Hg. v. xinhuanet.com. Online verfügbar unter http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm?utm_source=The+Sinocism+China+Newsletter&utm_campaign=d96724e196-Sinocism02_27_14&utm_medium=email&utm_term=0_171f237867-d96724e196-28921813, zuletzt aktualisiert am 14.04.2015, zuletzt geprüft am 14.04.2015.*

FALK GAENTZSCH,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen.

NORBERT POHLMANN,
Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen.