PROTECT-IT
FACHZEITSCHRIFT FÜR POLIZEI, ARMEE UND SICHERHEIT

Aus den Snowden-Enthüllungen

Der NSA-Skandal seit 2013

Die NAS gilt als mächtigster Hacker der Welt. Welche Daten sammelt die NSA, was ist Prism und wie reagieren die Überwachten? Seit Snowden seine Dokumente enthüllte hat sichj alles geändert – oder doch nicht? Ein Überblick seit Juni 2013.

Von June Carter

Brisant

- Die NSA hat jahrelang auch französische Spitzenpolitiker abgehört – darunter die Staatspräsidenten Sarkozy, Chirac und Hollande. Das belegen Dokumente, die WikiLeaks vor kurzem veröffentlicht hat.
- Die NSA und der britische Geheimdienst GCHQ haben die Hersteller von Antiviren-Software beobachtet und ihre Produkte durch *reverse engineering* untersucht. Ziel war es offenbar, Schwächen zu finden und diese für Angriffe auf Kunden ausnutzen zu können. Das geht aus Dokumenten aus dem Snowden-Archiv hervor, die *The Intercept* veröffentlicht hat. Die NSA hat im Projekt CAMBERDADA auch E-Mails abgefangen, in denen die Unternehmen auf mögliche neue Schadsoftware hingewiesen werden. Mindestens 23 Antivirus- und Sicherheitsfirmen sind oder waren betroffen. Die amerikanischen Antivirus-Firmen Symantec und McAfee sowie die britische Firma Sophos tauchen aber nicht in den Dokumenten auf.

Die Geschichte des Skandals

Im Juni 2013 begannen der britische *Guardian* und die amerikanische *Washington Post*, geheime Dokumente zu veröffentlichen, die sie vom früheren NSA-Mitarbeiter Edward Snowden bekommen hatten. Wie die Kontaktaufnahme von Snowden und den beteiligten Journalisten ablief, steht hier. Snowden selbst wurde in den USA der Spionage angeklagt und floh nach Russland ins Exil. Die beiden Zeitungen wurden im April 2014 für ihre Enthüllungen mit dem Pulitzer-Preis ausgezeichnet.

Die von Snowden entwendeten Dokumente enthüllen ein weltweites Netz von Spionagesystemen. Sie zeigen, dass die amerikanische National Security Agency (NSA), die britischen Government Communications Headquarters (GHCQ) und ihre Partnerdienste jede Form elektronischer Kommunikation überwachen wollen. Die wichtigsten Fakten im Überblick:

Wer überwacht, spioniert und hackt: Im Zentrum des Skandals stehen die NSA und der britische Geheimdienst GCHQ. Zu den engsten Partnern der USA und Grossbritannien gehören Kanada, Australien und Neuseeland, zusammen bilden sie die Five Eyes.

Weitere Länder arbeiten mit diesen fünf zusammen, darunter, Schweden, Frankreich, Belgien oder auch Japan und Südkorea. Sie alle profitieren von den Erkenntnissen insbesondere der Five Eyes und liefern ihnen eigene Informationen.

Wer überwacht, ausspioniert und gehackt wird:

- 122 Regierungschefs aus aller Welt, deren Telefongespräche die NSA abhört
- darunter auch Bundeskanzlerin Merkel und möglicherweise das ganze Berliner Regierungsviertel
- und vielleicht sogar ganz Deutschland – zumindest hat das zuständige US-Sondergericht die NSA am 7. März 2013 dazu autorisiert, wie der *Spiegel* berichtete
- Dass auch Deutsche von der massenhaften Datensammlung der NSA betroffen sind, legen zudem Dokumente nahe, die von der dänischen Zeitung *Dagbladet Information* und *The Intercept* veröffentlicht wurden und die die mehr als 50 Snowden-Dokumenten mit Deutschland-Bezug ergänzen, die der *Spiegel* ins Netz gestellt hat.
- alle US-Bürger. Die NSA sammelte von Oktober 2001 bis Mai 2015 sämtliche Verbindungsdaten aus Telefongesprächen und E-Mail-Verkehr in den USA. Am 1. Juni 2015 jedoch ist Sektion 215 des Patriot Acts ausgelaufen, die umstrittene rechtliche Grundlage für die Datenspeicherung.
- Millionen von Spaniern, Franzosen und Norwegern – jedenfalls haben die Geheimdienste dieser Länder der NSA jeweils Millionen von Verbindungsdatensätzen übergeben. Sie behaupten aber, es seien Daten aus der Auslandsaufklärung etwa in Afghanistan.
- Der belgische Telekommunikationsanbieter Belgacom, zu dessen Kunden auch das EU-Parlament, die EU-Kommission und der Europäische Rat gehören. Er wurde vom britischen Geheimdienst GCHQ gehackt.
- Staatsoberhäupter und ranghohe Politiker sowie mindestens ein Öl-Unternehmen in Brasilien und Mexiko
- Die Botschaften unter anderem von Frankreich, Italien, Griechenland sowie in EU-Vertretungen in den USA
- Google und Yahoo im Rahmen des Muscular-Programms, mit dem sich die NSA in die Verbindung zwischen den Rechenzentren der Unternehmen hackte
- Weltbank und der IWF
- Die Opec
- Indonesische Sicherheitsbehörden während der UN-Klimakonferenz 2007 auf Bali

- unbescholtene britische Staatsbürger, und zwar sowohl von der NSA als auch vom eigenen Geheimdienst GCHQ
- Einzelne muslimische Prediger, die mit Informationen über ihren Pornokonsum im Internet diskreditiert werden sollten
- Der ehemalige israelische Ministerpräsident Ehud Olmert, sein Verteidigungsminister, deutsche Regierungsgebäude im In- und Ausland, das deutsche Behördennetz, der EU-Wettbewerbskommissar, mehrere afrikanische Politiker sowie Organisationen wie Unicef und Médicins du Monde
- Möglicherweise der US-Kongress
- Politiker aus aller Welt vor dem Klimagipfel von Kopenhagen im Jahr 2009 und dem Klimagipfel von Cancún 2010.
- Jeder Mensch, der sich an bestimmten kanadischen Flughäfen ins kostenlose WLAN eingeloggt hat
- Die Anonymous-Bewegung
- Die Kommunikation einer US-Anwaltskanzlei mit der indonesischen Regierung
- WikiLeaks und die Nutzer der Seite *wikileaks.org*
- Millionen private Webcams von Yahoo-Nutzern
- Sämtliche Telefongespräche der jeweils vergangenen 30 Tage in Afghanistan und auf den Bahamas, sowie sämtliche Telefonmetadaten in Mexiko, Kenia und auf den Philippinen
- Kunden des französischen Providers Orange
- Der ehemalige chinesische Staatspräsident Hu Jintao, das chinesische Handelsministerium, das Aussenministerium, Banken sowie Telekommunikationsunternehmen wie Huawei
- Laut Snowden auch Menschenrechtsgruppen wie Amnesty International oder Human Rights Watch
- Nutzer der Anonymisierungssoftware Tor, Besucher der Website des Tor-Projekts und Menschen, die sich im Internet über Tor informieren.
- Unschuldige Internetnutzer, deren Mails oder Chats als "Beifang" anfallen, wenn die NSA Kommunikationshalte auf Grundlage von Sektion 702 des Fisa-Ergänzungsgesetzes abfängt. Nach Schätzungen der *Washington Post*, die 160.000 solcher Inhalte analysiert hat, sind neun von zehn Menschen in den Datenbanken der NSA keine Verdächtigen. Ihre Daten – darunter ärztliche Unterlagen, Babyfotos und Nacktbilder – bleiben demnach oft selbst dann gespeichert, wenn NSA-Analysten sie als nutzlos klassifizieren.
- Muslime, darunter auch Politiker, Rechtsanwälte und Bürgerrechtler, allesamt mit US-Staatsbürgerschaft.
- Somalia, Afghanistan und der Nahe Osten, hier sammelt der BND laut *Spiegel* sowohl Verkehrsdaten als auch Kommunikationsinhalte und bereitet die Daten im Bayerischen Bad

Aibling für die NSA auf – mithilfe von "15 bis 20 funktional unterschiedlichen Systemen" des US-Geheimdienstes.

- Neuseeland, hier hat der Geheimdienst GCSB laut Glenn Greenwald und Ryan Gallagher von *The Intercept* nach 2012 ein System zur massenhaften Metadatenüberwachung im Land installiert.
- 63 Unterseekabel wurden im Jahr 2009 durch die GCHQ und behilfliche Unternehmen wie Cable & Wireless (gehört seit 2012 zu Vodafone) angezapft. Betroffen waren dadurch Internetnutzer aus aller Welt.
- Rechner und ganze Netzwerke vor allem in in Russland und Saudi-Arabien, Mexiko, Irland, Indien, Afghanistan, dem Iran, Belgien, Österreich und Pakistan, aber auch in Deutschland und Belgien (siehe oben unter dem Stichwort "Belgacom"). Möglich war all das über Jahre hinweg mit der Malware Regin, die von NSA und GCHQ entwickelt worden sein soll.
- Forschungsanlagen für Nukleartechnik, Finanzinstitute sowie Telekommunikations-, Luftfahrt-, Energie- und Nanotechnologie-Unternehmen. Sie alle wurden mithilfe von äusserst mächtigen Spionageprogrammen überwacht, die wahrscheinlich vom selben (NSA-)Team entwickelt wurde, das später auch für Stuxnet verwantwortlich war.
- Mitarbeiter des SIM-Karten-Herstellers Gemalto. NSA und GCHQ haben das Unternehmen gehackt und auch die private Korrespondenz von Mitarbeitern ausgespäht, um einen Weg zu finden, die SIM-Karten-Schlüssel abzufischen, die Gemalto unter anderem zur Verschlüsselung von Handygesprächen in seine Produkte integriert.
- Regierungsmitarbeiter und Antikorruptions-Aktivisten auf den Salomonen. Neuseelands Geheimdienst GCSB hat sie mit Hilfe von XKeyScore ausspioniert.
- Bewerber für den Direktorenposten der Welthandelsorganisation WTO aus Brasilien, Costa Rica, Ghana, Indonesien, Jordanien, Kenia, Mexiko and Südkorea .Auch sie wurden von Neusselands Geheimdienst überwacht.

Die Ziele: Die Geheimdienste wollen Verdächtige finden, die sie bisher nicht kannten. Dazu analysieren sie die vielen Metadaten, also wer wann mit wem in Kontakt steht. "Man braucht den Heuhaufen, um darin die Nadel zu finden", hat der ehemalige NSA-Direktor Keith Alexander das Prinzip beschrieben.

Die NSA und die GCHQ spionieren aber auch gezielt einzelne Unternehmen und Spitzenpolitiker aus. Es geht ihnen also nicht nur um die Terrorbekämpfung, sondern auch um die eigenen politischen und wirtschaftlichen Interessen.

Ein ganz anderes Ziel für die nächsten Jahre ist es, kommerzielle und andere Verschlüsselungssysteme zu brechen – mithilfe von Technik oder auch Spionen, die in Unternehmen

für Verschlüsselungstechnik eingeschleust werden sollen. Das geht aus einem *"mission statement"* für die Zeit von 2012 bis 2016 hervor, das die *New York Times* veröffentlicht hat.

Die Programme und Quellen von NSA und GCHQ im Überblick

Die Informationsquellen:

Die bisher bekannt gewordenen Programme von NSA und GCHQ zeigen, wie umfassend die Geheimdienste jede Form von elektronischer Kommunikation unterwandert haben. Die folgende Liste zeigt, welche Datenquellen mit welchen Methoden angezapft werden und wie die Programme intern heissen.

- Metadaten aus Telefongesprächen und E-Mail-Verkehr
- Kontaktdaten aus Millionen von Adressbüchern, sie stammen von E-Mail-Konten und Instant-Messaging-Accounts
- DISHFIRE: Millionen von SMS, die täglich abgegriffen und ausgewertet werden
- Daten von Smartphone-Apps wie *Angry Birds* oder Google Maps
- Hunderte Millionen Standortdaten von Mobiltelefonen
- TEMPORA: alles, was über die transatlantischen Glasfaserkabel in die USA geschickt wird
- Roaming-Router grosser Mobilfunkanbieter
- PRISM: Google, YouTube, AOL, Apple, Microsoft, Skype, Yahoo, Facebook und PalTalk müssen Nutzerdaten herausgeben, wenn sie vom Geheimgericht FSC dazu gezwungen werden
- Partnerdienste wie der deutsche BND, die Daten an die NSA weitergeben
- SQUEAKY DOLPHIN: Aktivitäten auf YouTube und Googles Blogger-Plattform Blogspot sowie Facebook-Likes
- COTTONMOUTH, DROPOUTJEEP, RAGEMASTER: Verschiedene Wanzen und Hardware-Implantate in USB-Steckern, Kabeln und anderem Zubehör sowie Spionagesoftware für die gezielte Überwachung von Verdächtigen

- Radar zur Wohnraumüberwachung, mit dem sich sogar Bildschirminhalte erkennen lassen
- MUSCULAR: Datenverkehr zwischen den Rechenzentren von Google und Yahoo, in den sich die NSA gehackt hat
- 50.000 Netzwerke auf der ganzen Welt

- manipulierte Verschlüsselungstechnik sowie Hacks von verschlüsselten Verbindungen, Schwächung von krpytografischen Standards und Ausnutzen von Schwächen in bestehenden Verschlüsselungstechniken (LONGHAUL, BULLRUN, SCARLETFEVER, POISONNUT u.a.)
- Einzelne Smartphones, weil die NSA Hintertüren zu allen grossen Betriebssystemen kennt
- Grosse Teile des internationalen Zahlungsverkehrs
- Online-Plattformen wie *World of Warcraft* und *Second Life*
- Google-Cookies
- QUANTUM: Dateninjektion über NSA-eigene Server, die sich zwischen einen Nutzer und seine eigentliche Ziel-Website schalten
- HAMMERCHANT und HAMMERSTEIN zur Überwachung von VoIP-Gesprächen und Virtual Private Networks (VPN)
- Bilder, die übers Internet verschickt werden, sammelt die NSA millionenfach ein, um Verdächtige anhand von Gesichtserkennungstechnik zu identifizieren
- XKEYSCORE: Analyse- und Suchsoftware um Informationen über einzelne Menschen aus den riesigen Datenbanken der NSA zusammenzustellen. Wird auch von BND und Verfassungschutz benutzt.
- RAMPART-A: Programm der NSA, in dessen Rahmen weltweit wichtige Glasfaserkabel und Router angezapft werden, um Telefongespräche, Faxe, Mails, Chats, VoIP und andere Daten analysieren zu können. 13 Stellen, an denen diese Daten abgegriffen werden , gibt es weltweit. Eine davon befindet oder befand sich offenbar in Deutschland. Hier haben NSA, BND und ein unbekannter dritter Partner – wahrscheinlich ein Telekommunikationsunternehmen – im Rahmen des Unterprogramms WHARPDRIVE kooperiert.
- MINIATURE HERO: Echtzeit-Überwachung von Skype-Gesprächen, eines von vielen Werkzeugen des britischen Geheimdienstes GCHQ zur Überwachung und auch Manipulation von Computern und Internetinhalten.
- MonsterMind: Abwehr von Internetattacken auf die USA. Das 2013 noch nicht fertige System soll massenweise Metadaten im Netz analysieren, um normalen Traffic von Angriffen zu unterscheiden, diese zu lokalisieren und zu blockieren. Ausserdem kann MonsterMind nach unbelegten Angaben von Edward Snowden so programmiert werden, dass es sofort und automatisch zurückschlägt, wenn es einen Angriff erkennt.
- HACIENDA, LANDMARK, UPSHOT: Portscans in ganzen Ländern und Identifizierung anfälliger Server, die für weitere Angriffe übernommen werden können
- ICREACH: Suchmaschine der NSA, mit der 23 US-Behörden (darunter FBI und DEA) auf Metadaten in den NSA-Datenbanken zugreifen können.
- TREASURE MAP: Ein gemeinsames Programm von NSA und GCHQ, um das gesamte Internet zu kartografieren. Ziel ist es, jede einzelne Netzverbindung zu Endgeräten wie

Smartphones, Tablets und Rechnern nahezu in Echtzeit sichtbar machen zu können, um Computerattacken und Netzwerkspionage zu planen. Zu diesem Zweck dringen die Geheimdienste in fremde Netze ein, betroffen sind laut *Spiegel* neben mindestens 13 Anbietern im Ausland auch die Deutsche Telekom, Netcologne und die deutschen Unternehmen Stellar, Cetel und IABG, die in schwer zugänglichen Regionen etwa in Afrika Internetverbindungen via Satellit zur Verfügung stellen.

- Eikonal: Gemeinsame Operation von BND und NSA. Die Deutschen fingen zwischen 2004 und 2008 – angeblich mit Hilfe der Deutschen Telekom – Telefon- und Internetdaten in Frankfurt ab und leiteten die Rohdaten an die US-Amerikaner weiter. Auch Daten von Bundesbürgern waren dabei, weil die Filter des BND nicht richtig funktionierten. So stellten es jedenfalls die *Süddeutsche Zeitung*, NDR und WDR dar und beriefen sich auf streng geheime Akten des NSA-Ausschusses des Bundestages. Ein BND-Mitarbeiter wiedersprach dem bei seiner Befragung allerdings.
- TAREX (Target Exploitation): Programm der NSA, die offenbar auch in Deutschland Agenten stationiert hat, die Postpakete abfangen und die darin enthaltenen elektronischen Geräte verwanzen, bevor sie an den eigentlichen Empfänger gehen.
- Regin: extrem augefeilte Malware(-Familie), mit der jahrelang Rechner und ganze Netzwerke ausgespäht wurden. Laut *The Intercept* ist Regin ein Produkt von NSA und GCHQ.
- Hintertüren in Hardware: Der *Spiegel* kennt einen vierseitigen, als geheim eingestuften Bericht aus dem Jahr 2005, nach dem der BND damals auf eine US-Firma aufmerksam geworden war, die in Deutschland Hightech-Überwachungsanlagen mit Hintertüren für US-Geheimdienste anbot. Das Unternehmen versuchte demnach "zielgerichtet" seine Produkte in sicherheitsempfindlichen Bereichen wie "Rüstungsunternehmen und Hightech-Unternehmen in Konkurrenzposition zu US-Unternehmen, Ministerien, Sicherheitsbehörden" zu platzieren. In einem Labortest eines Mustergeräts stellten BND-Spezialisten fest, dass die Technik über das Internet ferngesteuert werden konnte.
- AURORAGOLD: Die NSA überwacht Mitarbeiter von Mobilfunkunternehmen in aller Welt, um Schwachstellen in deren Netzen ausfindig zu machen. Auf diese Weise hatte sich der Geheimdienst bis 2012 zumindest teilweisen Zugang auf 70 Prozent aller Mobilfunknetze verschafft.
- Operation Glotaic: zeitlich befristete Kooperation von CIA und BND bei der Überwachung ausländischer Telefonverbindungen in Deutschland
- LEVITATION: Kanadas Geheimdienst CSE scannt täglich zehn bis 15 Millionen Uploads und Downloads in frei zugänglichen Plattformen wie Sendspace, Rapidshare und dem mittlerweile abgestellten Megaupload nach Terrorverdächtigen und ihren Plänen.
- RHINEHART und SPIRITFIRE: Systeme, mit denen die NSA mitgeschnittene Telefongespräche automatisiert in Text umwandeln und nach Schlagworten durchsuchen konnte bzw. kann.

- CAMBERDADA: Projekt der NSA, um Informationen über neue Malware abzufangen und diese für Angriffe zu nutzen.

Weitere NSA-Programme und ihre Codenamen hat die Seite Electrospaces gesammelt. Die Bürgerrechtsbewegung ACLU hat alle bisher veröffentlichten Snowden-Dokumente durchsuchbar aufgelistet. Die französische Bürgerrechtsorganisation La Quadrature du Net hat unter *nsa-observer.net* eine Liste der knapp 300 bisher bekannten NSA-Überwachungsprogramme zusammengestellt.

Reaktionen und politische Folgen

Die Reaktionen in den USA:

Politisch hat sich seit Beginn der Enthüllungen nicht viel getan. Zwar hat zunächst eine offiziell unabhängige Expertengruppe die Praktiken der NSA unter die Lupe genommen und dem US-Präsidenten Barack Obama 46 Änderungsvorschläge unterbreitet. Aber bisher hat es nur zwei gesetzliche Neuerungen gegeben. Eine ist eher positiv zu werten, die andere eher negativ:

Am 1. Juni 2015 lief Abschnitt 215 des Patriot Acts aus, der seit Oktober 2001 die (umstrittene) rechtliche Grundlage für die Sammlung aller Telefonverbindungsdaten der US-Bürger bildete. Am 3. Juni ist dafür der USA Freedom Act inkraft getreten, der die Datenspeicherung neu regelt. Nicht mehr die NSA hält die Daten nun (nach einer Übergangsfrist von maximal 180 Tagen) vor, sondern die Provider. Die Regierung muss beim Foreign Intelligence Surveillance Court (Fisc) eng gefasste Anträge stellen, um Daten einsehen und analysieren zu dürfen. Auch darf die NSA nur noch die Daten von Kontakten von Verdächtigen analysieren, nicht mehr von Kontakten von Kontakten von Verdächtigen (*two hops* statt *three hops*). Geheime Interpretationen von Gesetzen durch den Fisc soll es nicht mehr geben. Der oberste Geheimdienstdirektor muss Entscheidungen des Gerichts, in denen Gesetze gedeutet werden, darauf prüfen, ob sie komplett oder in Teilen veröffentlicht werden können. Das neue Gesetz erlaubt es dem Fisc zudem, externe Experten anzuhören, um sich zum Beispiel technische Vorgänge und deren Auswirkungen auf die Privatsphäre von Überwachungszielen erklären zu lassen. Der USA Freedom Act enthält allerdings mehrere Ausnahmen und Sonderfälle, die einige der Neuerungen gleich wieder abschwächen.

Ende 2014 hat der Kongress zudem einen Gesetzentwurf verabschiedet, der die Befugnisse der NSA noch ausbaut, statt sie einzudämmen.Entscheidend ist Absatz 309 im Intelligence Authorization Act for Fiscal Year 2015: Darin geht es um "unabsichtlich" und ohne richterliche Beschlüsse erlangte Telefon- und Internetdaten von Ausländern und US-Bürgern. Diese Daten dürfen US-Geheimdienste

künftig maximal fünf Jahre aufbewahren, mit zahlreichen Ausnahmen. Handelt es sich zum Beispiel um verschlüsselte Kommunikation, gilt die Fünf-Jahres-Grenze nicht mehr. Es gibt bereits seit 1981 die präsidiale Verfügung 12333, nach der die Geheimdienste das alles schon dürfen – ohne irgendeine parlamentarische Kontrolle. Der Kongress hat die Befugnisse aus dieser Verfügung in Gesetzesform gegossen, sich dabei aber keine Kontrollmöglichkeit eingeräumt. Dianne Feinstein, die Vorsitzende des Geheimdienstausschusses des Senats hatte offenbar dafür gesorgt, dass der Passus nach einer ersten Abstimmung im Repräsentantenhaus nachträglich in den Entwurf geschrieben wurde. Dann hat der Senat den Entwurf abgesegnet. Anschliessen hat auch das Repräsantantenhaus der veränderten Fassung zugestimmt – vermutlich, ohne die Änderung bemerkt oder verstanden zu haben. Das Gesetz trat nach der Unterschrift von Präsident Obama am 19. Dezember 2014 inkraft.

Mehrere Bürgerrechtsorganisationen wie die EFF klagen seit Jahren gegen die NSA-Praktiken – auch die Wikimedia Foundation. Deren Begründung lautet: Die Internetüberwachung der NSA verletzte die Rechte von Wikipedia-Nutzern, insbesondere die verfassungsmässig garantierten Rechte auf Privatsphäre und Meinungsfreiheit.

Die wohl grössten Veränderungen gibt es auf technischer Ebene: Unternehmen wie Google, Apple und Microsoft bauen nach und nach ihre Verschlüsselungstechniken aus, um die Daten ihrer Kunden besser zu schützen. Der Anteil an verschlüsselten Internetverbindungen hat sich in den vergangenen zwölf Monaten weltweit deutlich erhöht. Das macht die Massenüberwachung durch Geheimdienste mindestens aufwendiger und teurer.

In Deutschland: Die Bundesregierung hat erst scharf auf die Enthüllungen reagiert, als klar war, dass auch die Bundeskanzlerin ein Ziel der NSA ist. Angela Merkel rief US-Präsident Barack Obama an und verlangte "Aufklärung über den Gesamtumfang" der US-Spionage in Deutschland. Der damalige Aussenminister Guido Westerwelle bestellte den US-Botschafter ein. Wirklich geändert hat sich seitdem aber wenig:

- Das Ziel, ein No-Spy-Abkommen mit den USA abzuschliessen, hat die Bundesregierung nicht erreicht. Der hier dokumentierte Schriftwechsel belegt, dass sie die Öffentlichkeit über den Verlauf der Gespräche absichtlich im Unklaren gelassen hat.
- Ein Parlamentarischer Untersuchungsausschuss soll "Ausmass und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären.
- Generalbundesanwalt Harald Range ermittelt wegen der Ausforschung des Handys von Angela Merkel, nicht aber wegen des Verdachts auf die massenhafte Überwachung der Bundesbürger. Die bisher veröffentlichten Dokumente reichen Range dazu nicht aus.

Mehrere deutsche Bundesbürger haben juristische Schritte eingeleitet, um gegen die Überwachung durch in- und ausländische Geheimdienste vorzugehen.

- Der Chaos Computer Club, der Verein digitalcourage und die Internationale Liga für Menschenrechte haben über die Berliner Rechtsanwälte Schultz & Förster beim Generalbundesanwalt eine 59 Seiten umfassende Strafanzeige "wegen verbotener Geheimdiensttätigkeit, Verletzung des persönlichen Lebens- und Geheimbereichs sowie Strafvereitelung" eingereicht. Sie richtet sich gegen "US-amerikanische, britische und deutsche Geheimdienstagenten und ihre Vorgesetzten", die Präsidenten des Bundesnachrichtendienstes, des Bundesamtes für Verfassungsschutz und des Militärischen Abschirmdienstes, gegen die Leiter der Landesämter für Verfassungsschutz, Bundeskanzlerin Angela Merkel, Bundesinnenminister Thomas de Maiziére, die übrigen Mitglieder der Bundesregierung "sowie die Amtsvorgänger der Beschuldigten."
- Der Berliner Anwalt Niko Härting hat vor dem Bundesverwaltungsgericht gegen die E-Mail-Überwachung des BND geklagt. Laut Jahresbericht des Parlamentarischen Kontrollgremiums hat der Bundesnachrichtendienst im Jahr 2010 rund 37 Millionen Mails durchsucht, sei dabei aber nur zwölf Mal auf "nachrichtendienstlich relevantes" Material gestossen. Härting geht davon aus, dass auch eine anwaltliche Korrespondenz betroffen gewesen sein könnte, weil die 37 Millionen nur die engere Auswahl gewesen seien. Die tatsächliche Zahl der durchsuchten Mails sei also grösser gewesen. Härting hält das für exzessiv und rechtswidrig. Das Gericht wies seine Klage aber ab. Der Anwalt will nun vors Bundesverfassungsgericht ziehen.
- Bürgerrechtler, darunter CCC-Sprecherin Constanze Kurz, haben den britischen Geheimdienst GCHQ wegen der umfassenden, verdachtsunabhängigen Überwachung von Millionen von EU-Bürgern vor dem Europäischen Gerichtshof für Menschenrechte verklagt.
- Wiederum der Chaos Computer Club sowie Privacy International und die Internet-Provider Riseup Networks, GreenNet, Greenhost, Mango, Jinbonet und May First/People Link gehen gegen die anlasslose Massenüberwachung von Internetnutzern durch den britischen Geheimdienst GCHQ vor. Sie haben dazu eine Beschwerde beim zuständigen Investigatory Powers Tribunal in Grossbritannien eingelegt.

Grossbritannien: Die parlamentarische Aufsicht über die britischen Geheimdienste MI5, MI6 und GCHQ ist schwach und ineffektiv. So steht es im Bericht des Ausschuss für innere Angelegenheiten im britischen Unterhaus, über den *heise.de* berichtet. In Zukunft soll für die Überprüfung der Geheimdienste nicht mehr nur der Geheimdienstausschuss zuständig sein. Allerdings hat die britische Regierung im Eilverfahren das DRIP-Gesetz durch das Parlament gebracht, das den Geheimdiensten nach Ansicht von Rechtsexperten neue Befugnisse verschafft und eine Vorratsdatenspeicherung wieder eindührt.

Amnesty International zieht gegen die britische Regierung wegen deren Massenüberwachungspraktiken vor den Europäischen Gerichtshof für Menschenrechte.

Österreich: Weil der BND im Auftrag der NSA möglicherweise auch österreichische Behörden ausspioniert hat, hat die österreichische Regierung Anzeige gegen Unbekannt erstattet.

Internationale Ebene: Das EU-Parlament hat den LIBE-Ausschuss beauftragt, den NSA-Skandal und seine Auswirkungen auf die EU-Bürger zu untersuchen. Der Ausschuss hat dazu Dutzende Experten angehört – darunter Techniker, Datenschützer, Aktivisten, Journalisten und Politiker. Der mit einigen Änderungen vom Ausschuss angenommene Entwurf des Abschlussberichts stellt die Legalität und das Ausmass der NSA-Überwachungsprogramme infrage, unterstellt der NSA auch Wirtschaftsspionage, verurteilt die anlasslose Massenüberwachung von Menschen in aller Welt und beinhaltet eine lange Liste von Forderungen. Die richten sich nicht nur gegen die USA, sondern auch gegen EU-Mitgliedstaaten – darunter auch Deutschland, das seine Geheimdienstgesetze überprüfen solle. Der Bericht wurde am 12. März vom Plenum angenommen.

Das EU-Parlament hat zudem eine Resolution verabschiedet, in der EU-Kommission und Ministerrat aufgefordert werden, das Swift-Abkommen auszusetzen. Es erlaubt den US-Behörden, unter bestimmten Voraussetzungen die Kontodaten europäischer Bürger abzufragen. Die EU-Kommission weist das Ansinnen des EU-Parlaments zurück und will weder das Swift-, noch das Fluggastdaten-Abkommen mit den USA stoppen.

Die UN-Vollversammlung hat im Dezember 2013 eine Resolution zum Schutz der Privatsphäre angenommen. Die Resolution geht auf einen Vorstoss von Deutschland und Brasilien zurück und ist eine direkte Reaktion auf die Spionageaffäre des US-Geheimdienstes NSA. Allerdings wurde die Resolution auf Druck der USA und der anderen Mitglieder der Five Eyes im Vorfeld abgeschwächt. Der Menschenrechtsausschuss der UN-Vollversammlung hat im November 2014 eine verschärfte Fassung gebilligt.

Frankreich im Spähnetz der NSA

Die NSA hört Frankreich ab

La Grande Nation empfand sich als besonderer Partner der USA. Merkel abgehört? Na ja… uns sicher nicht! Falsch gedacht! Was WikiLeaks nun über die NSA-Überwachung von französischen Spitzenpolitikern enthüllt hat, beinhaltet mehr als Handynummern und etwas Politspiele. Die Leaks

geben auch Auskunft über die mögliche Herkunft der Informationen und werfen die Frage auf, ob nicht sogar die Deutschen halfen, Sarkozy, François Hollande und den gesamten Regierungsapparat des Nachbarn auszuspionieren.

Die Quelle

Die Quelle für das WikiLeaks-Projekt "Espionnage Élysée" ist offenbar nicht Edward Snowden. WikiLeaks hat auch, anders als der *Guardian*, die *Washington Post* oder *Der Spiegel*, keine NSA-Originaldokumente veröffentlicht. Lediglich im begleitenden Artikel von *mediapart.fr* ist ein vollständiger Screenshot zu sehen. Die Liste der abgehörten Telefonnummern hat WikiLeaks in Form eines aufbereiteten Datenbankauszugs auf seine Website gestellt.

Die Ziele

Die Liste der abgehörten Telefonnummern beinhaltet einige Hinweise auf die Ziele der NSA. So steht hinter jeder Nummer eine Subscriber-ID, sie bezeichnet den Anschlussinhaber. Die von WikiLeaks veröffentlichte Liste beinhaltet das Handy der französischen Präsidenten, Nummern aus Ministerien und von Staatssekretären, Beratern und Sprechern. Manche Überwachungsaufträge reichen bis ins Jahr 2002 zurück und gelten zum Teil bis heute.

Zusätzliche Angaben verraten, dass die NSA unter anderem etwas über Frankreichs Afrika-Politik wissen wollte sowie über internationale Finanzpolitik. Damit belegen die Dokumente erneut, dass die NSA durchaus Wirtschaftsspionage betreibt, auch wenn sie es nicht auf Geschäftsgeheimnisse bestimmter Unternehmen abgesehen haben mag.

Die Verantwortlichen

Wer für die Abhöraktionen zuständig war, geht aus dem mit TOPI überschriebenen Feld im Datenbankauszug hervor. TOPI steht für Target Office of Primary Interest, der Begriff tauchte erstmals in einem vom *Guardian* veröffentlichten NSA-Dokument über die Zusammenarbeit mit Israel auf. Laut WikiLeaks bezeichnet er die für die Datenverarbeitung zuständige NSA-Einheit. Im Buch *Der NSA-Komplex* von den Spiegel-Autoren Marcel Rosenbach und Holger Stark sind TOPIs "die jeweilige Stelle innerhalb der NSA, die ein Ziel festlegt".

Im Datenbankauszug tauchen drei verschiedene TOPIs auf: S2C32, S2C13 und S2C51. Das erste – S2C32 – taucht in der Liste mehrfach auf und ist nicht ganz unbekannt. Dieselbe Einheit war für das Abhören von Angela Merkels Handy verantwortlich, damals als ROPI (Responsible Office of Primary

Interest), wie der *Spiege*l in seiner Ausgabe 44/2013 berichtete. Darin hiess es zur Erklärung: "S" steht für "Signal Intelligence Directorate", die Funkaufklärung der NSA. "2" ist die Abteilung für Beschaffung und Auswertung. C32 ist das zuständige Referat für Europa, die "European States Branch".

Die Methoden und mögliche Hilfe vom BND

Wie wurden die Gespräche abgehört? Dazu gibt es verschiedene Hinweise: Unter drei von fünf der veröffentlichten Gesprächszusammenfassungen steht die Anmerkung *Unconventional*. In seinem französischen Bericht definiert *Mediapart.fr* den Begriff als "Netzwerk-Piraterie", in einem englischen Artikel nur mit "erlangt durch nicht-konventionelle Operationen". Das könnten gezielte Hacks einzelner Telefone oder Provider sein. Unwahrscheinlich klingt das nicht. Die NSA und der britische Geheimdienst GCHQ haben mit ihrer Spionagesoftware Regin nicht nur den belgischen Telefonanbieter Belgacom gehackt, sondern auch mehrere andere Ziele in Europa.

In einem Fall (Sarkozy, 2008) steht an der entsprechenden Stelle nur *Unidentified*, die Abhörmethode ist also unbekannt. Unter dem Bericht über ein Telefonat von François Hollande aus dem Jahr 2012 steht ausserdem *Foreign Satellite, Unconventional*. *Foreign Satellite* heisst, die NSA hat hier nicht die eigenen Spionagesatelliten benutzt. Aber wessen dann? Es ist durchaus denkbar, dass auch hier der deutsche BND der NSA, wie in vielen anderen Fällen, bei der Spionage in Europa geholfen hat.

Partner der NSA

NSA und die Schweiz

Edward Snowdens Enthüllungen über die Überwachungsmethoden der Geheimdienste NSA und GCHQ kommen nach wie vor in regelmässigen Abständen und bringen Staaten und Unternehmen in Erklärungsnot. Die Schweiz war dabei immer nur am Rande betroffen, hat man bisher gedacht. Falsch, sagt die **Digitale Gesellschaft Schweiz**. Sie hat einen Bericht veröffentlicht, der die bisher bekannten Überwachungsmassnahmen in der Schweiz zusammenfasst. Es präsentiert sich ein Bild, das für rechtschaffene Bürger ziemlich erschreckend ist. Es gibt offenbar keine Möglichkeit, seine Daten vor fremdem Zugriff zu schützen.

Im Jahr 2000 verkaufte Swisscom die Satelliten-Bodenstation Leuk an die US-Gesellschaft Verestar, der Verbindungen zur NSA nachgesagt werden. Auf dem gleichen Gelände betreibt das

Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) Onyx, das elektronische Aufklärungssystem der Armee. Auch wenn diese Anlage nicht mitverkauft wurde, war schnell von Spionage die Rede. Mindestens ein Dienstleistungsvertrag wurde abgeschlossen, in dessen Rahmen sich Verestar – die heute Signalhorn AG heisst – um die Wartung der Infrastruktur von Onyx kümmern sollte. Kritische Stimmen wurden vom Bundesrat mit der Nachricht beschwichtigt, dass Verestar keine Kenntnisse von den VBS-Daten haben könne, weil das Unternehmen nicht mit klassifizierten Daten arbeitet.

Auch wenn diese wenig zufriedenstellende Antwort richtig sein sollte, stellt sich die Frage, ob die Schweiz der NSA erlauben soll, eine Abhöranlage zu betreiben. Laut geltendem Recht ist das Abfangen der Daten nur dann nicht erlaubt, wenn diese auf Schweizer Boden generiert werden oder innerhalb des Landes ausgetauscht werden, sagt das VBS. Gespräche oder Daten aus dem Ausland abzufangen sei ausländischen Nachrichtendiensten dagegen erlaubt. Falls also die NSA die Station Leuk als Spitzelposten für Deutschland nutzt, könnten die Schweizer Behörden nichts dagegen tun.

Botschaftsüberwachung

Gemäss einem Bericht von Edward Snowden betreibt die NSA weltweit 80 Abhörstationen in diplomatischen Vertretungen der USA. In der Schweiz soll sich eine in Genf auf dem Dach der amerikanischen UNO-Mission befinden. Die Genfer Abhörstation soll zudem vor Ort von Spezialisten betrieben werden. Das bedeutet, dass auch Einheiten des «Special Collection Service» (SCS) vor Ort sind, die Mobiltelefon, WLAN, Funk und Satellitenkommunikation abhören. Auch Edward Snowden gehörte einst zu diesem Team. «Weitere Einheiten dürften sich in der US-Botschaft in Bern sowie beim US-Konsulat in Zürich befinden», sagte ein ehemaliger NSA-Mitarbeiter der «Schweiz am Sonntag». Speziell in Zürich soll auch Abhörtechnik zum Einsatz kommen, die möglicherweise im Konsulat selbst stationiert ist. Laut dem NSA-Mitarbeiter sind die Amerikaner hier besonders an Informationen über den Finanzplatz interessiert. Zudem habe es die NSA von hier aus auch auf Zug abgesehen. Im Fokus stünden dort Rohstoffhandelskonzerne.

Dazu berichtet die Digitale Gesellschaft auch über den Schweizer Diplomaten Nicolas Imboden, der auf einer Überwachungsliste des britischen Geheimdienstes GCHQ gelandet ist. Dies, weil er in seiner Tätigkeit als Mitglied eines NGOs afrikanische Staaten im Kampf gegen hohe US-Baumwollsubventionen vertreten hat.

Zugriffsmöglichkeiten auf Schweizer Daten im Inland

Gemäss Edward Snowden zapft der GCHQ mit dem Programm «Tempora» im Wissen der Unternehmen Glaskabelverbindungen an. Zu den kooperierenden Firmen sollen mit British Telecom, Verizon und Level 3 Firmen gehören, die auch in der Schweiz Dienste anbieten. Ebenso wie Interroute und Viatel. Die «Weltwoche» deckte als Folge in einem Artikel auf, dass auch die Firma Equinix bei Tempora mitmischt. Diese hat hierzulande 7 Standorte und betreut drei grosse Internet-Knotenpunkte in der Schweiz. In einem der Rechenzentren von Equinix soll zudem der Server für den Aktienhandel der Schweizer Börse Six Swiss Exchange stehen.

Partner der NSA

Obwohl das VBS und insbesondere Ueli Maurer immer wieder betonen, dass die Schweiz sich an den NNSA-Aktivitäten nicht beteilige, geht aus einem Dokument Edward Snowdens das die spanische Zeitung «El Mundo» veröffentlicht hat, hervor, dass die Schweiz ein Kooperationspartner der NSA ist (Geheimdokument mit dem Titel «Sharing computer network operations cryptologic information with foreign partners»). Dabei handelt es sich um den Austausch verschlüsselter Daten mit ausländischen Partnern. In der Kategorie «Focused Cooperation» (enge Zusammenarbeit) taucht auch die Schweiz auf – neben Ländern wie Deutschland, Italien oder Spanien. «Focused Cooperation» beziehungsweise «Tier B» (Stufe B) ist die zweithöchste Stufe der Zusammenarbeit und die Gruppe umfasst 17 europäische Länder sowie Japan und Südkorea. Schweizer Behörden – vermutlich der Nachrichtendienst des Bundes (NDB) – arbeiten demnach Hand in Hand mit der NSA und zwar in amerikanischem Interesse. Die NSA profitiert unter davon, dass durch die Zusammenarbeit mit anderen Staaten das Überwachung von Kommunikation in Fremdsprachen erleichtert wird.