GERMAN-FOREIGN-POLICY.COM
Informationen zur deutschen Außenpolitik : Nachrichten + Interviews + Analysen + Hintergrund

Vorbild CIA 10.03.2017

BERLIN (Eigener Bericht) - Deutsche Geheimdienste sind seit geraumer Zeit mit der Beschaffung von Spionage- und Hackingtechnologien nach dem Modell der von WikiLeaks publizierten CIA-Programme befasst. Dies zeigen bekanntgewordene Informationen über aktuelle Projekte des BND und anderer Behörden. Demnach stehen dem Auslandsgeheimdienst bis 2020 rund 300 Millionen Euro zur Verfügung, um nicht nur die anlasslose Massenüberwachung von Internetkommunikation zu perfektionieren, sondern auch Software zum Eindringen in fremde Computer und Mobiltelefone zu entwickeln ("Strategische Initiative Technik"). Zudem will der Dienst im Rahmen eines 150-Millionen-Euro-Programms Möglichkeiten finden, Verschlüsselung unter anderem bei Messengern wie WhatsApp zu knacken oder zu umgehen. Erst vor wenigen Wochen hat Bundesinnenminister Thomas de Maizière eine Einrichtung gegründet, die dasselbe Ziel hat, aber mit ihrer Arbeit nicht den BND, sondern die Polizei und den Inlandsgeheimdienst ("Verfassungsschutz") bedient. Sie soll auf gut 400 Mitarbeiter aufwachsen und mit der Bundeswehr-Universität in München kooperieren. Bei der Bundeswehr wiederum sollen Kapazitäten für Cyberattacken auf jeder Eskalationsstufe entwickelt werden; diese übertreffen womöglich sogar die jetzt bekannt gewordenen Offensivfähigkeiten der CIA.

Der BND auf Aufholjagd

Die Aufrüstung der deutschen Geheimdienste mit Spionagetechnologien nach Art der CIA-Programme, die WikiLeaks publiziert hat, wird spätestens seit 2013 von Berlin vorangetrieben. Damals wurde durch den Whistleblower Edward Snowden die anlasslose Massenüberwachung durch die NSA bekannt und zum Skandal. Zudem erfuhr man, dass der BND nicht nur sehr eng mit der NSA kooperierte, sondern in Ermangelung hinlänglicher eigener Spionagekapazitäten auf diese Kooperation angewiesen war. "Das heißt, dass man vor zehn, 20 Jahren einen verheerenden strategischen Fehler gemacht hat, insofern man nicht ein gemeinsames europäisches Programm aufgelegt hat zur Entwicklung eigener Fähigkeiten", monierte damals der Politikwissenschaftler Herfried Münkler, ein Beiratsmitglied der Berliner Bundesakademie für Sicherheitspolitik (BAKS). Man müsse "hoffen", erklärte Münkler, "dass jetzt so schnell wie möglich entsprechende europäische Unternehmen damit beschäftigt werden, diese Fähigkeiten aufzubauen".[1] In der Tat hat die Bundesregierung die Haushaltsmittel für den BND umfassend aufgestockt. Erhielt er 2013 noch rund 530 Millionen Euro, so waren es 2015 schon 615 Millionen; im laufenden Jahr stehen dem Dienst bereits 808 Millionen Euro zur Verfügung.[2]

"Strategische Initiative Technik"

Das erste millionenschwere Projekt zur Weiterentwicklung der Internetspionage, das der BND bereits kurz nach Bekanntwerden der NSA-Massenüberwachung startete, läuft unter dem Namen "Strategische Initiative Technik".[3] Bis 2020 stehen dafür 300 Millionen Euro zur Verfügung. Gut 90 Prozent der Mittel werden, wie der Blog netzpolitik.org nach Auswertung interner Dokumente berichtet, für "Erfassung" und "Detektion nachrichtendienstlich relevanter Entwicklungen im Internet" aufgewandt.[4] Dazu zähle nicht nur die "anlasslose Massenüberwachung ganzer Kommunikationswege", so etwa zentraler Glasfaserverbindungen. Der BND bemühe sich auch darum, "Zugangsparameter" und "Software-Schwachstellen" in Erfahrung zu bringen. In einem BND-Strategiepapier werden ausdrücklich "Exploits für IT-Operationen" aufgelistet; dabei handelt es sich um Software, die es ermöglicht, in fremde Computer, Mobiltelefone und andere Geräte einzudringen. Im Rahmen der "Strategischen Initiative Technik" sucht der BND sich zudem in die Lage zu versetzen, in Echtzeit soziale Netzwerke wie Facebook oder Twitter zu durchforsten. Zu deren automatisierter Beobachtung hat er Berichten zufolge eine Studie an der Universität der Bundeswehr in München in Auftrag gegeben.[5]

"ANISKI"

Ein weiteres umfangreiches BND-Projekt zur Kommunikationsüberwachung ist im vergangenen Jahr bekannt geworden. Es trägt das Kürzel "ANISKI" ("Aufklärung nicht-standardisierter Kommunikation im Internet") und soll mit 150 Millionen Euro finanziert werden. Wie das Portal netzpolitik.org ebenfalls unter Berufung auf interne Dokumente berichtet, geht es dabei zentral um das Knacken von Verschlüsselung.[6] Weil diese mittlerweile bei vielgenutzten Onlinediensten, etwa bei Messengern wie WhatsApp, standardmäßig angewandt wird, sei man bei der Spionage "stark beeinträchtigt", erklärt laut netzpolitik.org der BND; man könne gegenwärtig "von aktuell weit über 70 verfügbaren Kommunikationsdiensten mit entsprechender Verbreitung" leider "nur weniger als zehn (zumeist ältere) erfassen und inhaltlich erschließen". Um dies zu ändern, müssten nun "Schwachstellen in der Implementierung" gefunden werden, wozu man auch "externe Firmen und Dienstleister" heranziehen wolle. Darüber hinaus wolle man sich bemühen, benutzte Schlüssel zu beschaffen. Letzteres solle "mit nachrichtendienstlichen Mitteln" geschehen, etwa mit "IT-Operationen und HUMINT-Operationen". Mit "IT-Operationen" ist das Hacken fremder Computer, Mobiltelefone oder anderer Geräte gemeint, mit "HUMINT-Operationen" ("Human Intelligence") die Spionage mittels V-Männern oder Agenten.[7]

Nicht nur der BND

Die technologische Aufrüstung à la CIA beschränkt sich dabei nicht auf den BND. Erst im Januar ist eine neue Einrichtung geschaffen worden, die sich ebenfalls vor allem mit dem Knacken von Verschlüsselung respektive dem Abfangen von Nachrichten noch vor der Verschlüsselung befasst: die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). Sie ist ohne das übliche Errichtungsgesetz auf Anordnung von Bundesinnenminister Thomas de Maizière etabliert worden und soll nicht selbst spionieren, sondern den interessierten Behörden wie der Bundespolizei, dem Bundeskriminalamt oder dem Inlandsgeheimdienst ("Verfassungsschutz") die nötige Technik zur Verfügung stellen. Der BND, der mit ANISKI seine eigenen Schritte eingeleitet hat, bleibt ZITis fern. Die Einrichtung hat mit gut 120 Mitarbeitern ihre Arbeit aufgenommen und soll bis 2022 auf rund 400 Mitarbeiter aufwachsen. Im aktuellen Bundeshaushalt stehen für ZITis bereits gut 12,5 Millionen Euro bereit.[8]

Cyberangriffe bei der Bundeswehr

ZITis ist in München angesiedelt worden und soll dort, wie das Bundesinnenministerium mitteilt, "perspektivisch" an die Universität der Bundeswehr angebunden werden, um "Ressourcen und Energie" zu bündeln. Dies bezieht sich auf das "Cyber Operational Defence" (CODE), das dort angesiedelt ist. CODE soll ab 2021/22 in neuen Gebäuden auf dem Universitätscampus untergebracht werden, in denen, wie es im Innenministerium heißt, auch der "Bedarf der ZITIS" gedeckt werden kann. "Die räumliche Nähe, der persönliche Austausch und informelle Treffen von spezialisierten Fachkräften fördern Innovation, Produktivität und Kreativität", heißt es dazu weiter.[9] Bei der Bundeswehr wiederum arbeitet man, wie im vergangenen Jahr bekannt wurde, daran, nicht nur Cyberangriffe abzuwehren, sondern auch "die gesamte Kette von Prävention zu Reaktion sowie von einfachen bis komplexen Angriffen ... [zu] beherrschen" (german-foreign-policy.com berichtete [10]). Dies übertrifft möglicherweise die Offensivfähigkeiten, über die laut den jüngsten WikiLeaks-Enthüllungen die CIA verfügt.

[1] Europäische Geheimdienste stärken. www.deutschlandradiokultur.de 26.10.2013.
[2] S. dazu **Vorbild NSA (II)** .
[3] S. dazu **Eine deutsch-europäische NSA** .
[4], [5] Andre Meister: Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will. netzpolitik.org 21.09.2015.
[6] Andre Meister: Projekt "ANISKI": Wie der BND mit 150 Millionen Euro Messenger wie WhatsApp entschlüsseln will (Update). netzpolitik.org 29.11.2016.
[7] Laut netzpolitik.org hat der BND schon zwischen 2003 und 2009 mehr als 2.500 mal fremde Computer gehackt.
[8] Martin Kaul: Backdoor im Gesetz. www.taz.de 09.11.2016.
[9] 24.1.2017 - Antwort vom BMI - ZITiS kommt zur Bundeswehr-Universität nach München. wiki.freiheitsfoo.de/pmwiki.php?n=Main.ZITiS#toc17 .
[10] S. dazu **Die Kriege der nächsten Jahre (IV)** .

Copyright © 2005 Informationen zur Deutschen Außenpolitik

info@german-foreign-policy.com