Geheimdienst-Aufrüstung stoppen!

Im Wortlaut von Jan Korte, 17. November 2014

Von Jan Korte, stellvertretender Vorsitzender der Fraktion DIE LINKE. im Bundestag

Durch die Enthüllungen von Edward Snowden wurde vor fast anderthalb Jahren klar: Der Überwachungsanspruch der Geheimdienste ist total. Eine effektive Kontrolle – weder parlamentarisch noch öffentlich – findet kaum statt, alles und jeder kann jetzt oder später mittels zahlloser Spionageprogramme ausgespäht werden. Die Bevölkerung steht unter Kollektivverdacht.

Doch wer gedacht hatte, dies würde zu einem Innehalten oder sogar einer Umkehr bei der Innen- und Sicherheitspolitik führen, sieht sich nicht nur ent- sondern getäuscht. Weder wurde das Agieren der Geheimdienste aufgeklärt noch etwas gegen die anlasslose Massenüberwachung unserer Kommunikation unternommen. Und nach einer kurzen Schamfrist gehen die Verfechter der Kontrollstaatsidee nun in die Offensive und verlangen die weitere Aufrüstung der Überwachungskapazitäten der Geheimdienste.

BND-Etat steigt und steigt

Nachdem die Koalitionsmehrheit im geheim tagenden Haushältergremium des Bundestages bereits im Mai dem Bundesnachrichtendienst (BND) für 2014 mehr als 6 Millionen Euro als erste Rate eines 300 Millionen Euro-Programms zur Vorbereitung seiner "Strategische Initiative Technik" (SIT) bewilligt hatte, wurde nun auch die Rate für das Jahr 2015 abgenickt:

Wie ZEIT Online berichtet soll der BND demnach bis 2020 für eine Liste von 26 Einzelprojekten insgesamt 300 Millionen Euro zusätzlich erhalten (ZEIT vom 13.11.2014), um "im Cyberbereich auf Augenhöhe mit den Partnern" (neues deutschland vom 11.6.2014) NSA und GHCQ zu kommen. Für 2015 wurden deshalb nun 28 Millionen Euro freigegeben, anschließend steigert sich die Aufrüstung Jahr für Jahr über 44 auf 58 Millionen. Insgesamt steigt der BND-Etat im nächsten Jahr um 56 Millionen gegenüber 2014.

Soziale Netzwerke sollen in Echtzeit analysiert werden

Der Ausbau der technischen Signalerfassung (SIGINT) schluckt dabei über die Hälfte der geplanten 300 Millionen Euro. Dadurch sollen die Dienste u.a. in die Lage versetzt werden das Kommunikationsverhalten von Nutzern sozialer Netzwerke in Echtzeit automatisiert analysieren und auswerten zu können. Nach Informationen der Süddeutschen Zeitung soll ein erster Prototyp zur Überwachung vor allem von Twitter und Blogs schon im Juni 2015 starten. Mittelfristig will der BND auch Facebook und andere Massen-Dienste ins Visier nehmen. Mit VIPER, dem mit 38 Millionen Euro teuersten Einzelprojekt sollen Verkehrsdaten und Inhalte gleichzeitig erfasst und analysiert werden (ZEIT ONLINE vom 13.11.2014). Die Echtzeit-Überwachung im Netz soll scheinbar auch durch das Teilprojekt der digitalen Aufrüstung

mit dem Codenamen "Nitidezza", für das BND-Präsident Gerhard Schindler 4,5 Millionen Euro ausgeben will, ermöglicht werden. Der BND hat bereits angekündigt, mit diesen Mitteln zukünftig auf dem Schwarzmarkt sogenannte Zero-Day-Exploits, also unveröffentlichte und nicht geschlossene Sicherheitslücken in Software, aufzukaufen, um diese zum Angriff auf Computersysteme zu benutzen. Ziel sei es künftig die Transportverschlüsselung SSL entschlüsseln, die auch zum Online-Banking und von vielen Shoppingportalen verwendet wird (vgl. SZ vom 10.11.2014).

Mit dem Wissen über Sicherheitslücken lassen sich seit etlichen Jahren riesige Profite erzielen. Statt die Sicherheitslücken an die Unternehmen zu melden, damit sie behoben werden, wird das geheime Wissen gegen bare Münze weiterverkauft. Im Zuge der Snowden-Enthüllungen wurde bekannt, dass die Geheimdienste offenbar die besten Kunden auf dem legalen wie dem illegalen Markt für Sicherheitslücken sind, den es ohne ihr Treiben in diesem Umfang sicher gar nicht gäbe. Allein die NSA gibt jährlich einen zweistelligen Millionenbetrag für Zero-Day-Exploits aus. 2012 soll sie sogar ein Jahresabo bei der französischen Firma Vupen, dem "Weltmarktführer für Schwachstellenforschung" abgeschlossen haben (vgl. Der Spiegel vom 10.11.2014). Union und SPD wollen offensichtlich, dass der BND verstärkt im Schwachstellen-Schwarzmarkt mitmischt. Folge? Deutsche Geheimdienste haben kein Interesse daran, dass eklatante Sicherheitslücken entdeckt werden. Die dadurch steigende Gefahr, dass die gleiche Sicherheitslücke auch anderen Geheimdiensten oder Kriminellen das Ausspähen von Staats- und Betriebsgeheimnissen erleichtert, nehmen die Geheimdienste und Regierungen willentlich in Kauf.

Geheimdienste unterlaufen durch Datentausch Kontrolle

Während kritische Sicherheitslücken also missbraucht werden sollen, um in Mobiltelefone und Computer einzubrechen, wird es gleichzeitig Bürgern und IT-Unternehmen erschwert, sich vor technischen Angriffen auf persönliche Daten oder Geschäftsgeheimnisse zu schützen. Doch damit nicht genug. Die Geheimdienstpraxis als Ganzes ist das Problem:

Sowohl die strategische Überwachung der grenzüberschreitenden Telekommunikation nach dem G 10-Gesetz als auch die strategische Überwachung der Telekommunikation im Ausland nach dem BND-Gesetz und die Nutzung von Daten, die von der NSA oder anderen Geheimdiensten deutschem Recht widersprechend gewonnen wurden, stehen im Verdacht der Verfassungswidrigkeit (vgl. die Sachverständigen Papier, Hoffmann-Riem und Bäcker im NSA-Untersuchungsausschuss am 22.05.2014). Insbesondere der "Daten-Ringtausch", den die Auslandsgeheimdienste betreiben, offenbart den Willen eine effiziente Kontrolle der eigenen Tätigkeit zu unterlaufen: Wer seine eigene Bevölkerung eigentlich nicht überwachen darf, bespitzelt eben einfach die Bevölkerung des anderen und tauscht anschließend die Daten mit dem Partnerdienst. Verfassung hin, Geheimdienstgesetz her.

Verbot des Aufkaufs von Zero-Day-Exploits durch Geheimdienste nötig

Mehr Sicherheit in der Informations- und Kommunikationstechnik kann es nur geben, wenn die Geheimdienste endlich ihr Treiben beenden. Wer gezielt Verschlüsselungsstandards unterwandert und Softwareschwachstellen ausnutzt und deshalb gegenüber NutzerInnen verschweigt, macht sich zur Gefahr für die IT-Sicherheit und zum unkontrollierbaren Risiko für sämtliche Nutzer des Netzes.

DIE LINKE fordert daher ein unverzügliches Verbot des Aufkaufs und der Verwendung von Zero-Day-Exploits durch Geheimdienste oder andere deutsche Behörden. Der Zuschuss an den BND darf nicht erhöht, sondern muss im Gegenteil um 50 Millionen Euro gekürzt werden. Außerdem soll der BND-Etat in den Folgejahren bis zum Zeitpunkt einer verfassungskonformen Neuregelung des G 10- und des BND-Gesetzes auf 400 Millionen Euro beschränkt werden.

Die eingesparten Gelder könnten dann endlich in eine gute personelle und materielle Ausstattung der Bundesdatenschutzbeauftragten und für die Auditierung von Open Source basierter Software fließen.

Wer um der Überwachung willen erheblichen Schaden im IT-Sektor in Kauf nimmt, sollte künftig gefälligst von Digitaler Agenda und IT-Sicherheit schweigen.

Die Geheimhaltung der Haushaltsvorlage des BND endet übrigens erst im Jahr 2074 … Dann dürfen die BürgerInnen nachlesen, warum BND und BfV sich von der NSA nur von der Größe, nicht aber vom Größenwahn her unterscheiden.

linksfraktion.de, 17. November 2014