Deutscher Bundestag **Drucksache 18/4267**

18. Wahlperiode 05.03.2015

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan van Aken, Christine Buchholz, Annette Groth, Ulla Jelpke, Kerstin Kassner, Niema Movassat und der Fraktion DIE LINKE.

Digitaler Jahrhundert-Bankraub und eine mutmaßliche Urheberschaft der Gruppe „Carbanak“

Eine Gruppe von Hackerinnen und Hackern mit dem Namen „Carbanak“ hat nach Medienberichten 1 Mrd. Dollar von rund 100 Finanzinstituten in 30 Ländern gestohlen (DIE WELT vom 15. Februar 2015). Aufgeklärt wurde der digitale Bankraub demnach vom IT-Sicherheitsunternehmen Kaspersky (IT – Informationstechnologie). Laut der Firma steckten „Cyberkriminelle aus Russland, der Ukraine, der EU und China“ hinter der Aktion, die über einen Zeitraum von zwei Jahren ausgeführt worden sei. Hierzu hätten die Hackerinnen und Hacker auf die Steuerung von Videokameras in Banken sowie Computer einzelner Mitarbeiterinnen und Mitarbeiter zugegriffen, unter anderem indem dort Trojaner-Programme installiert wurden. Zuvor seien die Täterinnen und Täter mit „Phishing-Methoden“ in Mailkonten eingedrungen. Dann seien „Rechner um Rechner“ auf die „Computer der Administratoren“ vorgedrungen. Dort hätten sie weitere „Remote Access Tools“ installiert um Passwörter mitzuschneiden. Je Bankraub seien „bis zu zehn Millionen Dollar“ erbeutet worden.

Angriffe seien auf Russland, die USA, China, Frankreich, Großbritannien, die Schweiz und Deutschland ausgeführt worden. Mindestens neun Banken in Deutschland seien betroffen. Kaspersky habe die Aktivitäten gemeinsam mit den Polizeiorganisationen INTERPOL und Europol entdeckt und aufgeklärt. Demnach seien bei den Aktivitäten „modifizierte Standardprogramme wie Metasploit oder Fernwartungssoftware wie TeamViewer“ benutzt worden. Die Ermittlerinnen und Ermittler machten sich zunutze, dass im Winter 2013 in Kiew verdächtige Aktivitäten an einem Bank-Automat aufgezeichnet worden seien. Die Bank habe schließlich „die Experten von Kaspersky“ mit Ermittlungen beauftragt. Möglicherweise seien aber die IT-Dienstleister Fox-IT und GroupIB im Jahr 2014 ebenfalls auf „einen Ring, der etwa 50 russische Banken angegriffen hatte“ gestoßen. Damals sei ein Trojaner namens „Anunak“ genutzt worden.

Wir fragen die Bundesregierung:

1. Welche Bundesbehörden und – soweit die Bundesregierung hierüber Kenntnis hat – auch Landesbehörden waren oder sind in die Ermittlungen gegen die Gruppe „Carbanak“ bzw. ähnlicher Aktivitäten eingebunden?
2. Wann und von wem waren welche deutschen Behörden erstmals über entsprechende Aktivitäten von „Carbanak“ oder ähnlicher Gruppen informiert bzw. aufmerksam gemacht worden?

3. Was ist der Bundesregierung darüber bekannt, welche internationalen Polizeibehörden ebenfalls an gemeinsamen Ermittlungen teilnehmen?
4. Was ist der Bundesregierung darüber bekannt, welche Firmen oder Institute ebenfalls an gemeinsamen Ermittlungen teilnehmen?
5. Inwiefern existieren oder existierten nach Kenntnis der Bundesregierung eigene Arbeitsgruppen internationaler oder deutscher Ermittlerinnen und Ermittler bzw. Firmen zu den Aktivitäten von „Carbanak“, und welche Details kann die Bundesregierung hierzu mitteilen?
6. Über welche eigenen Erkenntnisse verfügt die Bundesregierung über die Gruppe „Carbanak“?
7. Welche Finanzinstitute bzw. sonstigen Einrichtungen sind demnach in Deutschland betroffen (bitte nach Bundesländern aufschlüsseln)?
8. Welche Finanzinstitute bzw. sonstigen Einrichtungen sind nach Kenntnis der Bundesregierung demnach in welchen anderen Ländern betroffen?
9. Inwiefern kann die Bundesregierung die Schätzungen von Medien bestätigen, wonach rund 1 Mrd. Dollar gestohlen worden sein soll?
10. Inwiefern treffen nach Kenntnis der Bundesregierung Medienberichte bzw. Verlautbarungen des IT-Sicherheitsunternehmens Kaspersky zu oder nicht zu, wonach hinter den Aktivitäten „Cyberkriminelle aus Russland, der Ukraine, der EU und China“ steckten?
11. Inwiefern trifft es nach Kenntnis der Bundesregierung zu oder nicht zu, dass die Hackerinnen und Hacker auf die Steuerung von Videokameras in Banken sowie Computer einzelner Mitarbeiterinnen und Mitarbeiter zugegriffen haben?
12. Inwiefern trifft es nach Kenntnis der Bundesregierung zu oder nicht zu, dass auch Trojaner-Programme installiert wurden, und um welche Programme handelt es sich dabei?
13. Wie viele Personen wurden nach Kenntnis der Bundesregierung bereits als mutmaßliche Urheberinnen und Urheber der Hacks ermittelt?
14. Was ist der Bundesregierung über eine „Equation Group“ bekannt, und inwiefern bzw. mit welchen Behörden ist sie selbst in entsprechende Ermittlungen eingebunden (Süddeutsche Zeitung vom 17. Februar 2015)?
15. Inwiefern waren oder sind Einrichtungen in Deutschland nach Kenntnis der Bundesregierung von Aktivitäten der „Equation Group“ betroffen, und um welche handelt es sich dabei?
16. Welche Bundesbehörden und – soweit die Bundesregierung hierüber Kenntnis hat – auch Landesbehörden waren oder sind in die Ermittlungen gegen Botnetze, die Rechner angeblich mit der Malware „Ramnit“ infizieren, eingebunden (heise.de vom 25. Februar 2015)?
    a) Wann und von wem waren welche deutschen Behörden erstmals über entsprechende Aktivitäten informiert bzw. aufmerksam gemacht worden?
    b) Was ist der Bundesregierung darüber bekannt, welche internationalen Polizeibehörden ebenfalls an gemeinsamen Ermittlungen teilnehmen?
    c) Was ist der Bundesregierung darüber bekannt, welche Firmen oder Institute ebenfalls an gemeinsamen Ermittlungen teilnehmen?
    d) Worin genau bestand nach Kenntnis der Bundesregierung der Beitrag der Unternehmen Microsoft, Symantec und Anubisnetworks?

e) Inwiefern existieren oder existierten nach Kenntnis der Bundesregierung eigene Arbeitsgruppen internationaler oder deutscher Ermittlerinnen und Ermittler bzw. Firmen zu den Aktivitäten, und welche Details kann die Bundesregierung hierzu mitteilen?

17. Auf welche Weise ist es „Ermittlern der Polizeiorganisation Europol“ nach Kenntnis der Bundesregierung gelungen, „die Command-and-Control-Server ausfindig zu machen und vom Netz zu nehmen“?

18. Auf welche Weise sollen nach gegenwärtigem Stand „Nutzer in Deutschland, deren Computer unter der Kontrolle der Botnetz-Betreiber waren“, ermittelt und informiert werden, und um wie viele Betroffene handelt es sich vermutlich?

19. Nach welchem technischen Verfahren will die Bundesregierung PNR-Daten (Passenger Name Record – PNR) und Reisebewegungen von Personen einer „retroaktiven Analyse“ unterziehen, um wie gewünscht „weitere hilfreiche Ermittlungsansätze“ zu erhalten oder „bisher unbekannte Verbindungen zwischen Personen [zu] verdeutlichen“ (Bundestagsdrucksache 18/2972)?

a) Welche bereits vorhandene Software wäre hierfür geeignet?

b) Welche Art von Software könnte oder müsste hierfür beschafft werden?

20. Welche Methoden (außer Software) werden bei Bundesbehörden genutzt, um Finanzströme bzw. verdächtige Aktivitäten bei Kredit- und Finanzinstituten rückwirkend zu analysieren?

21. Welche Software wird bei Bundesbehörden genutzt, um Finanzströme bzw. verdächtige Aktivitäten bei Kredit- und Finanzinstituten rückwirkend zu analysieren?

22. Wie will die Bundesregierung technisch und organisatorisch umsetzen, dies, wie vom EU-Rat gefordert, weiter auszubauen (http://t.co/UzrCCPORDN)?

23. Was kann die Bundesregierung zu Herstellern bzw. Programmierern der bei Europol bereits genutzten „Ma^{3}tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit mitteilen (Bundestagsdrucksache 18/3910)?

24. Was kann die Bundesregierung zur Funktionsweise der bei Europol bereits genutzten „Ma^{3}tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit mitteilen?

25. Auf welche Weise wird bei „Ma^{3}tch“ ein „automatisierter oder anlassloser Datenaustausch“ vorgenommen (Bundestagsdrucksache 18/2888)?

26. Welche Abteilung des Bundeskriminalamtes (BKA) ist derzeit damit befasst, zu prüfen, ob die bei Europol bereits genutzte „Ma^{3}tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit auch beim BKA genutzt werden könnte (Bundestagsdrucksache 18/3910)?

a) Welche konkreten Fragen bzw. Annahmen liegen dieser Prüfung zugrunde?

b) Welche weiteren Behörden oder sonstigen Akteure sind an der Prüfung beteiligt?

c) Wann ist nach gegenwärtigem Stand mit einem Abschluss der Prüfung zu rechnen?

Berlin, den 4. März 2015

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333