Deutscher Bundestag **Drucksache 18/4437**

18. Wahlperiode 25.03.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/4267 –

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

Vorbemerkung der Fragesteller

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.

Vorbemerkung der Bundesregierung

In der Antwort zu Frage 14 sind Auskünfte enthalten, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Tätigkeit besonders schutzbedürftig sind, da diese im Zusammenhang mit den technischen Fähigkeiten der Nachrichten-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 23. März 2015 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

dienste stehen. Eine Kenntnisnahme von Informationen zu technischen Fähigkeiten der Nachrichtendienste durch Unbefugte könnte erhebliche nachteilige Auswirkungen auf deren operative Arbeit haben. In der Konsequenz entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland. Die künftige Aufgabenerfüllung der Nachrichtendienste des Bundes würde stark beeinträchtigt. Insofern könnte die Offenlegung der entsprechenden Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die Antworten zu den genannten Fragen als Verschlusssache gemäß der Verschlusssachenanweisung (VSA) mit dem Geheimhaltungsgrad „Geheim“ eingestuft.

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?

Nach Kenntnis der Bundesregierung führen aktuell keine deutschen Behörden Ermittlungen in Bezug auf die Schadsoftware „Carbanak“, da bislang keine Deutschlandbezüge bekannt geworden sind.

2. Wann und von wem waren welche deutschen Behörden erstmals über entsprechende Aktivitäten von „Carbanak“ oder ähnlicher Gruppen informiert bzw. aufmerksam gemacht worden?

Das Bundeskriminalamt (BKA) wurde erstmalig am 28. Oktober 2014 durch Europol über die Malware „Carbanak“ informiert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde erstmals Anfang November 2014 von CERT-EU über „Carbanak“ informiert.

3. Was ist der Bundesregierung darüber bekannt, welche internationalen Polizeibehörden ebenfalls an gemeinsamen Ermittlungen teilnehmen?

Der Bundesregierung liegen keine Erkenntnisse über gemeinsame Ermittlungen deutscher Strafverfolgungsbehörden mit internationalen Polizeibehörden in dieser Sache vor.

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?

Die Fragen 4 und 5 werden gemeinsam beantwortet.

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

6. Über welche eigenen Erkenntnisse verfügt die Bundesregierung über die Gruppe „Carbanak“?

Nach Kenntnis der Bundesregierung handelt es sich bei „Carbanak“ primär um die Bezeichnung einer Schadsoftware, die über den Standardfunktionsumfang

bekannter Schadsoftware verfügt (Ausschalten von Anti-Viren-Software, Fernzugriff, sogenannte Key-Logging- und Screen-Capture-Funktionalität). Weiterhin soll „Carbanak“ in der Lage sein, spezielle firmeninterne Bankenapplikationen festzustellen, um diese auszuforschen und anschließend zu missbrauchen. Zu möglichen Tätern liegen der Bunderegierung keine Erkenntnisse vor.

7. Welche Finanzinstitute bzw. sonstigen Einrichtungen sind demnach in Deutschland betroffen (bitte nach Bundesländern aufschlüsseln)?

Nach Kenntnis der Bundesregierung sind bisher keine deutschen Finanzinstitute oder sonstige Einrichtungen von der Schadsoftware „Carbanak“ betroffen.

8. Welche Finanzinstitute bzw. sonstigen Einrichtungen sind nach Kenntnis der Bundesregierung demnach in welchen anderen Ländern betroffen?

Bislang liegen der Bundesregierung nur Informationen zu Angriffen auf osteuropäische Finanzinstitute (fünf Banken in Russland und fünf Banken in der Ukraine) vor.

9. Inwiefern kann die Bundesregierung die Schätzungen von Medien bestätigen, wonach rund 1 Mrd. Dollar gestohlen worden sein soll?

Nach Kenntnis der Bundesregierung haben zwei der angegriffenen Banken einen Gesamtwert von ca. 17 Mio. US-Dollar verloren.

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?

Die Fragen 10 und 11 werden gemeinsam beantwortet.

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

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?

Der Bundesregierung liegen die Analyseberichte von Kaspersky und F-Secure/GroupIB vor. Demnach wurde bei „Carbanak“ eine Abwandlung der „Caberp“-Malware verwendet. Dabei handelt es sich um einen Trojaner, der bisher eingesetzt wurde, um einzelne Online-Banking-Nutzer anzugreifen.

13. Wie viele Personen wurden nach Kenntnis der Bundesregierung bereits als mutmaßliche Urheberinnen und Urheber der Hacks ermittelt?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

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)?

Die Antwort auf den ersten Teil der Frage ist als Verschlusssache gemäß der VSA mit dem Geheimhaltungsgrad „Geheim“ eingestuft.* Hierzu wird auf die Vorbemerkung der Bundesregierung verwiesen.

Zum zweiten Teil der Frage: Die Analyse des Sachverhalts wird in einer Arbeitsgruppe des Nationalen Cyber-Abwehrzentrums durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und das BSI durchgeführt.

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?

Eine mögliche deutsche Betroffenheit wird von einer Arbeitsgruppe im Nationalen Cyber-Abwehrzentrum geprüft.

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)?

Nach Kenntnis der Bundesregierung ist in Deutschland nur das BKA in die Ermittlungen gegen das Ramnit-Botnetz eingebunden gewesen. In Deutschland befanden sich relevante Server. Zur Umsetzung der Maßnahmen wurde eine zuständige Staatsanwaltschaft in Sachsen eingebunden.

a) Wann und von wem waren welche deutschen Behörden erstmals über entsprechende Aktivitäten informiert bzw. aufmerksam gemacht worden?

Das BKA wurde durch Europol am 12. November 2014 erstmalig über international geplante Maßnahmen in Kenntnis gesetzt. Das BSI wurde am 6. Februar 2015 vom BKA über die für den 24. Februar 2015 geplante Abschaltung der für das Ramnit-Botnetz relevanten Server-Infrastruktur informiert.

b) Was ist der Bundesregierung darüber bekannt, welche internationalen Polizeibehörden ebenfalls an gemeinsamen Ermittlungen teilnehmen?

Die Abschaltung des Ramnit-Botnetzes wurde von der europäischen Polizeibehörde Europol in Den Haag international koordiniert. Italien, die Niederlande und Großbritannien waren ebenfalls beteiligt.

c) Was ist der Bundesregierung darüber bekannt, welche Firmen oder Institute ebenfalls an gemeinsamen Ermittlungen teilnehmen?

Nach Kenntnis der Bundesregierung waren die Unternehmen Microsoft, Anubis Networks und Symantec an der koordinierten Aktion gegen das Ramnit-Botnetz beteiligt.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

d) Worin genau bestand nach Kenntnis der Bundesregierung der Beitrag der Unternehmen Microsoft, Symantec und Anubisnetworks?

Nach Kenntnis der Bundesregierung sind die benannten Firmen bei der Identifizierung der täterseitig genutzten Infrastruktur sowie in Bezug auf die Bereinigungsbemühungen infizierter Endgeräte eingebunden gewesen.

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?

Nach Kenntnis der Bundesregierung ist die bei Europol eingerichtete Joint Cybercrime Action Task Force die einzige Arbeitsgruppe mit „internationalen oder deutschen Ermittlern“. Diese war in die Koordinierung der Maßnahmen eingebunden.

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“?

Da operative Maßnahmen der Hoheit einzelner Staaten gemäß nationalem Recht obliegen, wurde die Server-Infrastruktur durch die ermittelnden nationalen Behörden identifiziert, die auch die hoheitlichen Maßnahmen im jeweils eigenen Land durchführten. Es wurden keine eigenen „Ermittler der Polizeiorganisation Europol“ eingesetzt. Europol hatte nur eine koordinierende Rolle, wie auch den Pressemitteilungen von BKA und Europol zu entnehmen ist.

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?

Die mit einem Schadprogramm infizierten Computersysteme versuchen in der Regel, mit einem Kontrollserver Kontakt aufzunehmen. Seit der Abschaltung der Botnetz-Infrastruktur werden diese Verbindungsanfragen protokolliert. Das BSI erhält vom CERT-EU seit dem 25. Februar 2015 in unregelmäßigen Abständen entsprechende Informationen über IP-Adressen in Deutschland. Diese werden an die jeweils zuständigen Provider weitergeleitet mit der Bitte, die Kunden über die vermutete Infektion ihrer PCs zu informieren.

Das BSI geht mit Stand 10. März 2015 von ca. 600 bis 1 000 Infektionen in Deutschland aus.

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?

Die Fragen 19, 19a und 19b werden gemeinsam beantwortet.

Entsprechende Überlegungen hat die Bundesregierung noch nicht angestellt. Welche konkreten technischen Verfahren oder welche Softwareprodukte zur Analyse der PNR-Daten zur Anwendung kommen könnten, wird abhängig vom weiteren Fortgang der Verhandlungen über die PNR-Richtlinie zu gegebener Zeit zu betrachten sein.

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

Das BKA und der Zollfahndungsdienst verwenden für Finanzermittlungen in konkreten Ermittlungsverfahren die bei Banken nach den Möglichkeiten der Strafprozessordnung erhobenen Daten von Herkunfts- und Zielkonten für eine Geldflussanalyse. Dabei werden grundsätzlich nur die Daten genutzt, die im Rahmen eines Strafverfahrens erhoben wurden und als Beweismittel verwendet werden dürfen.

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

Für Finanzermittlungen kommen bei Bundesbehörden folgende Softwareprodukte zum Einsatz:

- Microsoft-Office-Anwendungen, insbesondere Excel,
- Analyst's Notebook (IBM),
- IDEA (CaseWare International Inc.), inkl. dem ergänzenden Analysewerkzeug AIS TaxAudit (Audicon GmbH),
- b-case als Fallbearbeitungssystem sowie rs-case für darüber hinausgehende Analysezwecke (Rola Securities).

Ergänzend wird auf die Antwort zu Frage 20 verwiesen.

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

Der Rat der Europäischen Union fordert in dem zitierten Papier: „Member States quickly implement the strengthened rules to prevent money laundering and terrorist financing, and that all competent authorities step up action to trace financial flows and to freeze assets used for financing terrorism." Die Bundesregierung wird die Vorgaben der Vierten Geldwäsche-Richtlinie fristgerecht umsetzen.

23. Was kann die Bundesregierung zu Herstellern bzw. Programmierern der bei Europol bereits genutzten „Ma³tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit mitteilen (Bundestagsdrucksache 18/3910)?

Ansprechpartner und Programmierer der Ma³tch-Technologie ist das FIU.Net-Projekt:

FIU.NET Bureau

Dutch Ministry of Security and Justice

c/o Eisenhowerlaan 73

P.O. Box 90850

2509 LW Den Haag

The Netherlands

Die „Ma³tch“-Technologie wird bei Europol noch nicht genutzt. Eine Nutzung erfolgt durch das FIU.net. Es ist beabsichtigt, das FIU.Net-Projekt zu Europol zu überführen. Hierzu wird auf die Antwort zu Frage 19e auf Bundestagsdrucksache 18/2888 verwiesen.

24. Was kann die Bundesregierung zur Funktionsweise der bei Europol bereits genutzten „Ma³tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit mitteilen?

Nach Kenntnis der Bundesregierung handelt es sich bei der Ma³tch-Funktion um einen „automatisierten“ Abgleich pseudonymisierter Daten, nach dem Hit-No-Hit-Prinzip. Die pseudonymisierten Daten müssen dazu von den „Teilnehmern“ aktiv zur Verfügung gestellt werden. Vor einem Abgleich werden die Personendaten in Hashwerte umgewandelt. Die Ma³tch-Funktionalität ist keine fachliche Anwendung, um verdächtige Finanztransaktion aufzuspüren, weder in Echtzeit noch retrograd. Ergänzend wird auf die Antwort zu Frage 23 verwiesen.

25. Auf welche Weise wird bei „Ma³tch“ ein „automatisierter oder anlassloser Datenaustausch“ vorgenommen (Bundestagsdrucksache 18/2888)?

Zur Funktionsweise wird auf die Antwort zu Frage 24 verwiesen. Durch Artikel 53 Absatz 2 des Entwurfs der Vierten EU-Geldwäscherichtlinie (2013/0025(COD)) soll der auf der Ma³tch-Funktion basierte „anonyme“ Datenaustausch gesetzlich klargestellt werden:

„[…] Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs co-operate in the application of state-of-the-art technologies in accordance with their national law. Those technologies shall allow FIUs to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds.“

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?

Die Fragen 26, 26a und 26b werden gemeinsam beantwortet.

Die Prüfung beim BKA obliegt der Abteilung Schwere und Organisierte Kriminalität in Abstimmung mit anderen zuständigen Abteilungen. Die Prüfung erfolgt unter Maßgabe der vom FIU.NET erarbeiteten Vorgaben und Spezifikationen. Ergänzend wird auf die Antwort zu Frage 25 verwiesen.

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

Das BKA wird seine Prüfung voraussichtlich bis zum Sommer 2015 abschließen.

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

Deutscher Bundestag **Drucksache 18/4437**

18. Wahlperiode 25.03.2015

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/4267 –

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

Vorbemerkung der Fragesteller

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.

Vorbemerkung der Bundesregierung

In der Antwort zu Frage 14 sind Auskünfte enthalten, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Tätigkeit besonders schutzbedürftig sind, da diese im Zusammenhang mit den technischen Fähigkeiten der Nachrichten-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 23. März 2015 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

dienste stehen. Eine Kenntnisnahme von Informationen zu technischen Fähigkeiten der Nachrichtendienste durch Unbefugte könnte erhebliche nachteilige Auswirkungen auf deren operative Arbeit haben. In der Konsequenz entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland. Die künftige Aufgabenerfüllung der Nachrichtendienste des Bundes würde stark beeinträchtigt. Insofern könnte die Offenlegung der entsprechenden Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die Antworten zu den genannten Fragen als Verschlusssache gemäß der Verschlusssachenanweisung (VSA) mit dem Geheimhaltungsgrad „Geheim“ eingestuft.

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?

Nach Kenntnis der Bundesregierung führen aktuell keine deutschen Behörden Ermittlungen in Bezug auf die Schadsoftware „Carbanak“, da bislang keine Deutschlandbezüge bekannt geworden sind.

2. Wann und von wem waren welche deutschen Behörden erstmals über entsprechende Aktivitäten von „Carbanak“ oder ähnlicher Gruppen informiert bzw. aufmerksam gemacht worden?

Das Bundeskriminalamt (BKA) wurde erstmalig am 28. Oktober 2014 durch Europol über die Malware „Carbanak“ informiert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde erstmals Anfang November 2014 von CERT-EU über „Carbanak“ informiert.

3. Was ist der Bundesregierung darüber bekannt, welche internationalen Polizeibehörden ebenfalls an gemeinsamen Ermittlungen teilnehmen?

Der Bundesregierung liegen keine Erkenntnisse über gemeinsame Ermittlungen deutscher Strafverfolgungsbehörden mit internationalen Polizeibehörden in dieser Sache vor.

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?

Die Fragen 4 und 5 werden gemeinsam beantwortet.

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

6. Über welche eigenen Erkenntnisse verfügt die Bundesregierung über die Gruppe „Carbanak“?

Nach Kenntnis der Bundesregierung handelt es sich bei „Carbanak“ primär um die Bezeichnung einer Schadsoftware, die über den Standardfunktionsumfang

bekannter Schadsoftware verfügt (Ausschalten von Anti-Viren-Software, Fernzugriff, sogenannte Key-Logging- und Screen-Capture-Funktionalität). Weiterhin soll „Carbanak“ in der Lage sein, spezielle firmeninterne Bankenapplikationen festzustellen, um diese auszuforschen und anschließend zu missbrauchen. Zu möglichen Tätern liegen der Bunderegierung keine Erkenntnisse vor.

7. Welche Finanzinstitute bzw. sonstigen Einrichtungen sind demnach in Deutschland betroffen (bitte nach Bundesländern aufschlüsseln)?

Nach Kenntnis der Bundesregierung sind bisher keine deutschen Finanzinstitute oder sonstige Einrichtungen von der Schadsoftware „Carbanak“ betroffen.

8. Welche Finanzinstitute bzw. sonstigen Einrichtungen sind nach Kenntnis der Bundesregierung demnach in welchen anderen Ländern betroffen?

Bislang liegen der Bundesregierung nur Informationen zu Angriffen auf osteuropäische Finanzinstitute (fünf Banken in Russland und fünf Banken in der Ukraine) vor.

9. Inwiefern kann die Bundesregierung die Schätzungen von Medien bestätigen, wonach rund 1 Mrd. Dollar gestohlen worden sein soll?

Nach Kenntnis der Bundesregierung haben zwei der angegriffenen Banken einen Gesamtwert von ca. 17 Mio. US-Dollar verloren.

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?

Die Fragen 10 und 11 werden gemeinsam beantwortet.

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

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?

Der Bundesregierung liegen die Analyseberichte von Kaspersky und F-Secure/GroupIB vor. Demnach wurde bei „Carbanak“ eine Abwandlung der „Caberp“-Malware verwendet. Dabei handelt es sich um einen Trojaner, der bisher eingesetzt wurde, um einzelne Online-Banking-Nutzer anzugreifen.

13. Wie viele Personen wurden nach Kenntnis der Bundesregierung bereits als mutmaßliche Urheberinnen und Urheber der Hacks ermittelt?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

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)?

Die Antwort auf den ersten Teil der Frage ist als Verschlusssache gemäß der VSA mit dem Geheimhaltungsgrad „Geheim“ eingestuft.* Hierzu wird auf die Vorbemerkung der Bundesregierung verwiesen.

Zum zweiten Teil der Frage: Die Analyse des Sachverhalts wird in einer Arbeitsgruppe des Nationalen Cyber-Abwehrzentrums durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und das BSI durchgeführt.

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?

Eine mögliche deutsche Betroffenheit wird von einer Arbeitsgruppe im Nationalen Cyber-Abwehrzentrum geprüft.

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)?

Nach Kenntnis der Bundesregierung ist in Deutschland nur das BKA in die Ermittlungen gegen das Ramnit-Botnetz eingebunden gewesen. In Deutschland befanden sich relevante Server. Zur Umsetzung der Maßnahmen wurde eine zuständige Staatsanwaltschaft in Sachsen eingebunden.

a) Wann und von wem waren welche deutschen Behörden erstmals über entsprechende Aktivitäten informiert bzw. aufmerksam gemacht worden?

Das BKA wurde durch Europol am 12. November 2014 erstmalig über international geplante Maßnahmen in Kenntnis gesetzt. Das BSI wurde am 6. Februar 2015 vom BKA über die für den 24. Februar 2015 geplante Abschaltung der für das Ramnit-Botnetz relevanten Server-Infrastruktur informiert.

b) Was ist der Bundesregierung darüber bekannt, welche internationalen Polizeibehörden ebenfalls an gemeinsamen Ermittlungen teilnehmen?

Die Abschaltung des Ramnit-Botnetzes wurde von der europäischen Polizeibehörde Europol in Den Haag international koordiniert. Italien, die Niederlande und Großbritannien waren ebenfalls beteiligt.

c) Was ist der Bundesregierung darüber bekannt, welche Firmen oder Institute ebenfalls an gemeinsamen Ermittlungen teilnehmen?

Nach Kenntnis der Bundesregierung waren die Unternehmen Microsoft, Anubis Networks und Symantec an der koordinierten Aktion gegen das Ramnit-Botnetz beteiligt.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

d) Worin genau bestand nach Kenntnis der Bundesregierung der Beitrag der Unternehmen Microsoft, Symantec und Anubisnetworks?

Nach Kenntnis der Bundesregierung sind die benannten Firmen bei der Identifizierung der täterseitig genutzten Infrastruktur sowie in Bezug auf die Bereinigungsbemühungen infizierter Endgeräte eingebunden gewesen.

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?

Nach Kenntnis der Bundesregierung ist die bei Europol eingerichtete Joint Cybercrime Action Task Force die einzige Arbeitsgruppe mit „internationalen oder deutschen Ermittlern“. Diese war in die Koordinierung der Maßnahmen eingebunden.

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“?

Da operative Maßnahmen der Hoheit einzelner Staaten gemäß nationalem Recht obliegen, wurde die Server-Infrastruktur durch die ermittelnden nationalen Behörden identifiziert, die auch die hoheitlichen Maßnahmen im jeweils eigenen Land durchführten. Es wurden keine eigenen „Ermittler der Polizeiorganisation Europol“ eingesetzt. Europol hatte nur eine koordinierende Rolle, wie auch den Pressemitteilungen von BKA und Europol zu entnehmen ist.

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?

Die mit einem Schadprogramm infizierten Computersysteme versuchen in der Regel, mit einem Kontrollserver Kontakt aufzunehmen. Seit der Abschaltung der Botnetz-Infrastruktur werden diese Verbindungsanfragen protokolliert. Das BSI erhält vom CERT-EU seit dem 25. Februar 2015 in unregelmäßigen Abständen entsprechende Informationen über IP-Adressen in Deutschland. Diese werden an die jeweils zuständigen Provider weitergeleitet mit der Bitte, die Kunden über die vermutete Infektion ihrer PCs zu informieren.

Das BSI geht mit Stand 10. März 2015 von ca. 600 bis 1 000 Infektionen in Deutschland aus.

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?

Die Fragen 19, 19a und 19b werden gemeinsam beantwortet.

Entsprechende Überlegungen hat die Bundesregierung noch nicht angestellt. Welche konkreten technischen Verfahren oder welche Softwareprodukte zur Analyse der PNR-Daten zur Anwendung kommen könnten, wird abhängig vom weiteren Fortgang der Verhandlungen über die PNR-Richtlinie zu gegebener Zeit zu betrachten sein.

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

Das BKA und der Zollfahndungsdienst verwenden für Finanzermittlungen in konkreten Ermittlungsverfahren die bei Banken nach den Möglichkeiten der Strafprozessordnung erhobenen Daten von Herkunfts- und Zielkonten für eine Geldflussanalyse. Dabei werden grundsätzlich nur die Daten genutzt, die im Rahmen eines Strafverfahrens erhoben wurden und als Beweismittel verwendet werden dürfen.

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

Für Finanzermittlungen kommen bei Bundesbehörden folgende Softwareprodukte zum Einsatz:

- Microsoft-Office-Anwendungen, insbesondere Excel,
- Analyst's Notebook (IBM),
- IDEA (CaseWare International Inc.), inkl. dem ergänzenden Analysewerkzeug AIS TaxAudit (Audicon GmbH),
- b-case als Fallbearbeitungssystem sowie rs-case für darüber hinausgehende Analysezwecke (Rola Securities).

Ergänzend wird auf die Antwort zu Frage 20 verwiesen.

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

Der Rat der Europäischen Union fordert in dem zitierten Papier: „Member States quickly implement the strengthened rules to prevent money laundering and terrorist financing, and that all competent authorities step up action to trace financial flows and to freeze assets used for financing terrorism." Die Bundesregierung wird die Vorgaben der Vierten Geldwäsche-Richtlinie fristgerecht umsetzen.

23. Was kann die Bundesregierung zu Herstellern bzw. Programmierern der bei Europol bereits genutzten „Ma³tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit mitteilen (Bundestagsdrucksache 18/3910)?

Ansprechpartner und Programmierer der Ma³tch-Technologie ist das FIU.Net-Projekt:

FIU.NET Bureau

Dutch Ministry of Security and Justice

c/o Eisenhowerlaan 73

P.O. Box 90850

2509 LW Den Haag

The Netherlands

Die „Ma³tch“-Technologie wird bei Europol noch nicht genutzt. Eine Nutzung erfolgt durch das FIU.net. Es ist beabsichtigt, das FIU.Net-Projekt zu Europol zu überführen. Hierzu wird auf die Antwort zu Frage 19e auf Bundestagsdrucksache 18/2888 verwiesen.

24. Was kann die Bundesregierung zur Funktionsweise der bei Europol bereits genutzten „Ma³tch“-Technologie zum Aufspüren verdächtiger Finanz-Aktivitäten in Echtzeit mitteilen?

Nach Kenntnis der Bundesregierung handelt es sich bei der Ma³tch-Funktion um einen „automatisierten“ Abgleich pseudonymisierter Daten, nach dem Hit-No-Hit-Prinzip. Die pseudonymisierten Daten müssen dazu von den „Teilnehmern“ aktiv zur Verfügung gestellt werden. Vor einem Abgleich werden die Personendaten in Hashwerte umgewandelt. Die Ma³tch-Funktionalität ist keine fachliche Anwendung, um verdächtige Finanztransaktion aufzuspüren, weder in Echtzeit noch retrograd. Ergänzend wird auf die Antwort zu Frage 23 verwiesen.

25. Auf welche Weise wird bei „Ma³tch“ ein „automatisierter oder anlassloser Datenaustausch“ vorgenommen (Bundestagsdrucksache 18/2888)?

Zur Funktionsweise wird auf die Antwort zu Frage 24 verwiesen. Durch Artikel 53 Absatz 2 des Entwurfs der Vierten EU-Geldwäscherichtlinie (2013/0025(COD)) soll der auf der Ma³tch-Funktion basierte „anonyme“ Datenaustausch gesetzlich klargestellt werden:

„[…] Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs co-operate in the application of state-of-the-art technologies in accordance with their national law. Those technologies shall allow FIUs to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds.“

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?

Die Fragen 26, 26a und 26b werden gemeinsam beantwortet.

Die Prüfung beim BKA obliegt der Abteilung Schwere und Organisierte Kriminalität in Abstimmung mit anderen zuständigen Abteilungen. Die Prüfung erfolgt unter Maßgabe der vom FIU.NET erarbeiteten Vorgaben und Spezifikationen. Ergänzend wird auf die Antwort zu Frage 25 verwiesen.

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

Das BKA wird seine Prüfung voraussichtlich bis zum Sommer 2015 abschließen.

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