Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-1117
FAX +49 (0)30 18 681-1019

INTERNET www.bmi.bund.de

DATUM 14. April 2015

BETREFF **Kleine Anfrage des Abgeordneten Jan Korte u. a. und der Fraktion DIE LINKE.**

Konsequenzen nach Angriff auf weltweit größten Chipkarten-Hersteller durch die Geheimdienste NSA und GCHQ

BT-Drucksache 18/4530

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte Antwort in 4-facher Ausfertigung.

Hinweis:

Antworten der Kleinen Anfrage sind VS-NUR FÜR DEN DIENSTGEBRAUCH EINGESTUFT

Mit freundlichen Grüßen
in Vertretung

Dr. Ole Schröder

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
VERKEHRSANBINDUNG S-Bahnhof Bellevue; U-Bahnhof Turmstraße
Bushaltestelle Kleiner Tiergarten

Kleine Anfrage des Abgeordneten Jan Korte u. a. und der Fraktion DIE LINKE.

Konsequenzen nach Angriff auf weltweit größten Chipkarten-Hersteller durch die Geheimdienste NSA und GCHQ

BT-Drucksache 18/4530

Vorbemerkung der Fragesteller:

Bei dem Versuch, die weltweite Kommunikation überwachen und kontrollieren zu können, geraten zunehmend Internet-Sicherheitsfirmen ins Visier der Geheimdienste. Die Enthüllungsplattform „The Intercept" hat am 19. Februar 2015 Dokumente aus dem Fundus von Edward Snowden veröffentlicht, laut denen eine gemeinsame Hacker-Spezialeinheit des britischen Geheimdienst GCQH und des US-amerikanischen Geheimdienstes NSA die Verschlüsselungscodes für SIM-Karten des niederländischen Chip- und Magnetstreifenkarten-Herstellers Gemalto erbeutet haben soll (first-look.org/theintercept/2015/02/19/great-sim-heist/).

Demnach seien NSA und GCHQ im Jahr 2010 in die Systeme von Gemalto, der sich selbst als „Weltführer bei digitaler Sicherheit" bezeichnet, eingedrungen und hätten millionenfach SIM-Karten-Schlüssel gestohlen. Die Firma produziert neben SIM-Karten unter anderem auch Ausweise, Plastikgeld, Mobile-Payment-Geldbörsen, Autoschlüssel und die elektronische Gesundheitskarte. Laut „The Intercept" beinhalten die Snowden-Dokumente darüber hinaus Hinweise, dass die Geheimdienste 2010 auch einen vergleichbaren Angriff auf Gemaltos Konkurrenten, den deutschen Chiphersteller „Giesecke & Devrient", geplant hatten. Außerdem muss davon ausgegangen werden, dass in den vergangenen Jahren auch andere Hersteller Ziel geheimdienstlicher Angriffe waren. Ebenso werden in den von „The Intercept" analysierten Dokumenten mit Nokia, Huawei und Ericsson die zum damaligen Zeitpunkt großen Handyhersteller als Spionageziel genannt (vgl. hierzu auch www.heise.de/newsticker/meldung/SIM-Karten-Hack-Die-Kompromittierung-der-Mobilfunknetze-durch-NSA-GCHQ-2555714.html).

Durch den Diebstahl der Verschlüsselungscodes wäre es den Geheimdiensten möglich, unbemerkt massenhaft Handy-Kommunikation abzuhören - auch ohne Anfrage an die Provider oder einen Gerichtsbeschluss. Gemalto hat nach den Enthüllungen eine Untersuchung eingeleitet und die Ergebnisse am 25. Februar 2015 bekannt gegeben (www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx). Die Prüfung habe demnach ergeben, dass es höchstwahrscheinlich tatsächlich Cyber-Angriffe der Geheimdienste im Jahr 2010 gegeben habe, bei diesen sei allerdings nur in das Büronetz von Gemalto eingebrochen worden „und sie hätten nicht zu einem massiven Diebstahl von Sim-Karten-Schlüssel führen können", so die Stellungnahme. Zugleich ließ Gemalto jedoch die Möglichkeit offen, dass Sim-Karten-Schlüssel außerhalb der gesicherten Systeme des Konzerns abgegriffen worden sein könnten. Dem Bericht von „The Intercept" zufolge sollen die Geheimdienste versucht haben, die Codes bei der Übermittlung an Mobilfunk-Kunden abzufangen. Gemalto erklärte nun, dass die Firma allerdings bereits vor 2010 bis auf „wenige Ausnahmen" einen sicheren Übertragungsweg eingesetzt habe. Allerdings hätten laut Gemalto einige andere Anbieter und Mobilfunkbetreiber zum damaligen Zeitpunkt keine sicheren Übertragungswege benutzt. Gemalto teilte weiter mit, dass die Firma dank des Berichts von „The Intercept" schließlich Cyberattacken aus den Jahren 2010 und 2011 habe einordnen und dabei unter anderem feststellen können, dass damals eine französische Website des Konzerns ausgespäht und die Computer mehrerer Mitarbeiter angegriffen wurden. Ferner seien an einen Netzbetreiber E-Mails mit verseuchtem Anhang von angeblichen Gemalto-Adressen verschickt worden, was ebenfalls als Teil der Geheimdienst-Aktion eingeschätzt wird. „Giesecke & Devrient" erklärte hingegen, dass die Firma „bisher keine Erkenntnisse darüber, dass SIM-Karten-Schlüssel entwendet wurden" habe (vgl. SPON vom 25.02.2015). Unterdessen haben Sicherheitsforscher den Verdacht geäußert, dass die SIM-Karten-Schlüssel gar nicht das eigentliche Ziel der Geheimdienste waren und stattdessen die Angriffe das Ziel der Erbeutung der sogenannten OTA-Schlüssel (Over The Air) verfolgt habe. Mit den OTA-Schlüsseln können SIM-Karten-Updates aus der Ferne signiert werden und so wären Geheimdienste in der Lage, unbemerkt Spionagesoftware auf die SIM-Karte von Verdächtigen zu übertragen. Entsprechende Angriffs-Szenarien werden ebenfalls in einem der Snowden-Dokumente als mögliches Ziel erwähnt (vgl. (ZEIT Online vom 25.02.2015).

Durch das Kompromittieren des Gemalto-Firmen-Netzes könnten darüber hinaus insbesondere auch für das IT-Großprojekt elektronische Gesundheitskarte (eGK) neue und massive Sicherheitsgefahren entstanden sein. So lieferte alleine Gemalto in den vergangenen Jahren für die AOK, Deutschlands größter Krankenversicherung, u.a. ihr Produkt „Sealys eGK" an die 25 Millionen AOK-Mitglieder und übernahm dabei den gesamten Prozess der Kartenherstellung von der Produktion, über die Personalisierung bis hin zur Auslieferung (vgl. hierzu u.a. www.gemalto.com/press/Pages/news_1222.aspx).
Professor Hartmut Pohl, Mitglied des Beirats der International Security Academy und Sprecher des Präsidiumsarbeitskreises "Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e. V, schätzt, dass in Deutschland aktuell weit mehr als 50.000 der wichtigsten Server in Unternehmen, Regierung und Verwaltung (Strategic Servers) mit sogenannten Backdoors der NSA versehen sind (vgl. www.deutsche-gesundheitsnachrichten.de/2015/02/26/e-card-angst-vor-datenmissbrauch-ueberschattet-medizinischen-nutzen/).

Vorbemerkung:
Die Antwort auf die Kleine Anfrage beinhaltet zum Teil detaillierte Einzelheiten zu den technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen der Behörden. Aus ihrem Bekanntwerden könnten Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Ermittlungsbehörden gezogen werden. Deshalb sind einzelne Informationen gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) als „VS - NUR FÜR DEN DIENSTGEBRAUCH" eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.
Dies betrifft die Antworten zu den Fragen 4 und 10.

1. Welche Erkenntnisse hat die Bundesregierung seit welchem Zeitpunkt über den geheimdienstlichen Angriff auf den niederländischen Chip- und Magnetstreifen-Karten-Hersteller Gemalto?

Zu 1.
Der Sachverhalt ist der Bundesregierung über die Medienberichterstattung bekannt geworden. Eigene Erkenntnisse lagen zu diesem Zeitpunkt nicht vor. In der Folge sind verschiedene Maßnahmen ergriffen worden, um die Hintergründe und Auswirkungen des in Rede stehenden Angriffs aufzuklären. Im Einzelnen wird hierzu auf die Antwort zu Frage 10 verwiesen.

10. Welche Erkenntnisse hat die Bundesregierung seit welchem Zeitpunkt über einen möglichen geheimdienstlichen Angriff auf den deutschen SIM-Karten-Hersteller „Giesecke & Devrient"?

Zu 1.
Auf die Antwort zu Frage 1 wird verwiesen.

3. Revidiert die Bundesregierung nach Bekanntwerden des Gemalto-Hacks ihre Position, dass kein US-amerikanischer Geheimdienst deutsche Unternehmen und Konzerne ausspäht (vgl. Antwort auf Frage 5 der Kleinen Anfrage der Fraktion die LINKE auf Drucksache 18/2281)?

Zu 3.
Der Bundesregierung liegen zu dem fragegegenständlichen Sachverhalt keine eigenen Erkenntnisse vor. Sie sieht daher derzeit keine Veranlassung, frühere Aussagen zu revidieren.

4. Welche Ergebnisse hat die „Sonderauswertung Technische Aufklärung durch US-amerikanische, britische und französische Nachrichtendienste" des Bundesamtes für Verfassungsschutz (BfV) zur Überprüfung der Enthüllungen durch Edward Snowden in Bezug auf den Gemalto-Hack und ggf. weitere Angriffe auf Wirtschaftsunternehmen bis heute ergeben?

Zu 4.
Auf den „VS-NUR FÜR DEN DIENSTGEBRAUCH" eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung wird verwiesen.

5. Revidiert die Bundesregierung nach Bekanntwerden des Gemalto-Hacks ihre Antwort auf Frage 8 der Kleinen Anfrage der Fraktion die LINKE (Drucksache 18/2281), wonach sie keine Erkenntnisse zu Wirtschaftsspionage durch die NSA oder anderen US-Diensten in anderen Staaten habe und wenn ja in welcher Form? Wenn nein, warum nicht?

Zu 5.

Nein. Es liegen weiterhin keine Erkenntnisse zu angeblicher Wirtschaftsspionage durch die NSA oder anderen US-Diensten in anderen Staaten vor.

6. Wie schätzt die Bundesregierung die durch den Gemalto-Hack und mögliche weitere Angriffe befreundeter Geheimdienste auf IT-Sicherheitsunternehmen bestehende Bedrohungslage ein?

Zu 6.

Der Bundesregierung liegen keine Erkenntnisse vor, die hierzu eine Schlussfolgerung zuließen.

7. Teilt die Bundesregierung die Einschätzung von Professor Pohl, wonach in Deutschland aktuell weit mehr als 50.000 sogenannte Strategic Servers mit Backdoors der NSA versehen sind? Wenn ja, was gedenkt sie dagegen zu unternehmen? Wenn nein, zu welcher Einschätzung kommt die Bundesregierung und wie viele Strategic Servers sind nach Erkenntnissen der Bundesregierung durch die NSA und andere befreundete Nachrichtendienste kompromittiert?

Zu 7.

Eine Einschätzung, für wie viele strategisch relevante Server das Vorhandensein von Backdoors anzunehmen bzw. auszuschließen ist, ist nicht möglich.
Der Bundesregierung liegen keine Erkenntnisse zu kompromittierten Strategic Servern in Deutschland vor.

8. Hält die Bundesregierung, neben der Überwachungsproblematik, auch Identitätsdiebstahl, also das Täuschen mit falschen Identifizierungsnachweisen, als Folge des Gemalto-Hacks für möglich (Bitte begründen)?

Zu 8.

Nationale Identitätsdokumente sind vom „Gemalto-Hack“ nicht betroffen.
Ein Identitätsdiebstahl wäre jedoch bspw. möglich, wenn sich ein Nutzer nur über ein Mobiltelefon und die dortige SIM-Karte identifiziert. Bislang liegen der Bundesregierung keine Erkenntnisse zu einer solchen Begehungsweise vor.

9. Teilt die Bundesregierung die Auffassung, dass die internen Kontrollen und Sicherheitsüberprüfungen von Gemalto, angesichts der technischen Möglichkeiten der Geheimdienste, völlig unzureichend gewesen sind, wenn bis zu den Veröffentlichungen der entsprechenden Snowden-Dokumente dieses Datenleck den Betreibern der Firma nicht aufgefallen ist und welche Schlussfolgerungen zieht die Bundesregierung daraus?

Zu 9.
Es ist nicht Aufgabe der Bundesregierung, das Sicherheitsmanagement von Gemalto in Frankreich oder den Niederlanden zu bewerten.

10. Welche Maßnahmen haben Bundesregierung und deutsche Sicherheitsbehörden in Folge des geheimdienstlichen Angriffs von NSA und GCHQ auf den niederländischen SIM-Karten-Hersteller Gemalto wann in die Wege geleitet und welche Ergebnisse hatten diese jeweils?

Zu 10.
Auf den „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung wird verwiesen.

11. Welche Sicherheitsbehörden oder staatliche Stellen erfassen in welcher Form und aufgrund welcher Informationen und Meldewege die Häufigkeiten, Schwere und Konsequenzen von Cyber-Angriffen statistisch und wird dabei auch nach Angriffen durch Geheimdienste oder andere Cyber-Kriminelle differenziert?

Zu 11.
Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) erfasst alle relevanten IT-Angriffe und stellt diese im Rahmen regelmäßig erscheinender Lageberichte dar. Aussagen zu den möglichen Urhebern solcher IT-Angriffe erfolgen in Abstimmung unter anderem mit dem Bundesamt für Verfassungsschutz (BfV), dem Bundeskriminalamt (BKA) und der Bundespolizei (BPOL).

12. Was wurde nach Kenntnis der Bundesregierung von wem unternommen, um auszuschließen, dass Geräte noch „infiziert" sind?

Zu 12.
Die Einleitung entsprechender Maßnahmen obliegt allein Gemalto in Kooperation mit den dort zuständigen nationalen Behörden.

13. Wären, wenn sich bestätigen sollte, dass sich NSA und GCHQ „nur" in das Gemalto-Büronetz eingehackt haben, nach Einschätzung der Bundesregierung dann nur die über 10.000 Mitarbeiter von Gemalto betroffen?

Zu 13.
Der Bundesregierung liegen keine hinreichenden Erkenntnisse vor, um sich zu der Fragestellung äußern zu können.

14. Wie charakterisiert die Bundesregierung geheimdienstliche Angriffe auf Chip-Karten-Hersteller und hält sie eine strafrechtliche Verfolgung für geboten (Bitte begründen)?

Zu 14.
Ein nachrichtendienstlicher Angriff auf einen Chip-Kartenhersteller kann bei Vorliegen aller Voraussetzungen den Straftatbestand der Geheimdienstlichen Agententätigkeit nach § 99 Absatz 1 Nummer 1 des Strafgesetzbuchs (StGB) erfüllen. Hierzu bedarf es u. a. eines Tätigwerdens "gegen die Bundesrepublik Deutschland". Nach der Rechtsprechung des Bundesverfassungsgerichts erfasst dieses Tatbestandsmerkmal auch Umstände, in denen sich das Tätigwerden auf beliebige Tatsachen aus jedem Bereich, auch aus Wirtschaft und Wissenschaft bezieht (Az 2 BvR 215/81; Beschl. vom 26. Mai 1981; BVerfGE 57, 267, Rn. 43). Darunter können auch Angriffe auf Chipkartenhersteller fallen. Bei einem Angriff auf Informationssysteme kommt darüber hinaus eine Strafbarkeit nach § 202a StGB (Ausspähen von Daten) in Betracht. Danach macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.
Die Beurteilung der Frage, ob insoweit jeweils der für ein strafrechtliches Einschreiten erforderliche Anfangsverdacht gegeben ist, obliegt den zuständigen Strafverfolgungsbehörden.

15. Wird die Bundesregierung mögliche Versuche der betroffenen Firmen, Provider und Kunden unterstützen, die NSA sowie GCHQ bzw. die USA und Großbritannien auf Schadenersatz und Unterlassung zu verklagen? Wenn ja, in welcher Form? Wenn nein, warum nicht?

Zu 15.
Da sich die Hinweise auf die Meldungen über den Vorfall und auf eine konkrete nationale Gefährdung bislang nicht bestätigt haben, besteht derzeit kein Anlass für Überlegungen im Sinne der Fragestellung.

16. Hat sich die Bundesregierung in Folge der Veröffentlichungen mit der Forderung um Aufklärung an die Regierungen der USA und Großbritanniens gewandt und wenn ja, wann und in welcher Form und mit welchem Ergebnis passierte dies?

Zu 16.
Die Bundesregierung sieht derzeit keine Veranlassung, entsprechende Ersuchen an die Regierungen der beiden Staaten zu richten.

17. Hält die Bundesregierung für den Fall, dass sich die Angriffe auf IT-Sicherheitsfirmen wie Gemalto bestätigen und die USA sowie Großbritannien keine Aufklärung leisten und ihre Geheimdienste ihre entsprechenden illegalen Aktivitäten nicht einstellen, politische und wirtschaftliche Sanktionen für ein mögliches Mittel der Reaktion (Bitte begründen)?

Antwort zu Frage 17:
Die Bundesregierung äußert sich nicht zu hypothetischen Fragestellungen.

18. Welche Chip- und Magnetstreifenkarten-Produkte sind nach Kenntnis der Bundesregierung potentiell von dem Gemalto-Hack durch NSA und GCHQ betroffen?

Zu 18.
Der Bundesregierung liegen bisher lediglich die bekannten Presseinformationen vor. Zu Umfang und Ziel der mutmaßlichen Aktivitäten können daher keine Aussagen getroffen werden.
Da Chipkarten von Gemalto sowohl für Debit- als auch für Kreditkarten eingesetzt werden, könnten potenziell beide Kartenarten betroffen sein.

19. Hat die Bundesregierung Erkenntnisse darüber, dass das eigentliche Ziel der Angriffe die OTA-Schlüssel gewesen sind, um unbemerkt Spionagesoftware auf die SIM-Karten von Zielpersonen übertragen zu können? Wenn ja, welche sind dies?

Zu 19.
Der Bundesregierung liegen hierzu keine über die Presseberichterstattung hinausgehenden Erkenntnisse vor.

20. Welcher wirtschaftliche Schaden ist nach Erkenntnissen der Bundesregierung schätzungsweise dadurch entstanden?

Zu 20.
Der Bundesregierung liegen keine hinreichenden Erkenntnisse vor, die hier eine Einschätzung zuließen.

21. Welche Ministerien, Bundesbehörden und sicherheitsrelevanten Einrichtungen und Bereiche in der Bundesrepublik sind potentiell durch den Krypto-Schlüssel-Diebstahl in jeweils welchem Ausmaß betroffen?

Zu 21.
Die Regierungskommunikation ist nach aktueller Erkenntnislage nicht betroffen. Zum Schutz vertraulicher Informationen werden im Übrigen zusätzliche technische Sicherungsmaßnahmen genutzt.

22. Wie viele SIM-Karten welcher Modelle und welcher Telefongesellschaften und Telekommunikationsanbieter sind nach Kenntnis der Bundesregierung potentiell betroffen?

23. Wie viele EC-/Kredit-Karten welcher Modelle und welcher Banken sind nach Kenntnis der Bundesregierung potentiell betroffen?

Zu 22. und 23.
Der Bundesregierung liegen hierzu keine Informationen vor.

24. Wie viele eGK-Karten welcher Modelle und welcher Krankenversicherungen sind nach Kenntnis der Bundesregierung potentiell betroffen?

Zu 24.

Keine. Nach Kenntnis der Bundesregierung ist die eGK insgesamt nicht von dem beschriebenen Angriff betroffen.

25. Kann die Bundesregierung die Pressemeldung der Gematik vom 25.02.2015 bestätigen (www.e-health-com.eu/details-news/gematik-veroeffentlicht-stellungnahme-zum-versuchten-angriff-auf-kartenhersteller-gemalto/b93cf7591c081503b74de1d4e40c5798/) und definitiv ausschließen, dass von dem Angriff der Geheimdienste der USA und Großbritanniens auf den Kartenhersteller Gemalto elektronische Gesundheitskarten nicht betroffen sind?

Zu 25.

Die Bundesregierung hat keine Erkenntnisse, die Zweifel an der Darstellung der Gematik aufkommen lassen. Im Übrigen werden für die eGK technisch und organisatorisch andere Sicherheitskonzepte und -verfahren genutzt.

26. Wie viele Pässe und Personalausweise welcher Staaten sind nach Kenntnis der Bundesregierung jeweils potentiell betroffen?

Zu 26.

Im Umfeld deutscher hoheitlicher Dokumente wie Reisepässe oder Personalausweise werden keine Chips des Unternehmens Gemalto verwendet. Die Beschlüsselung der hierfür verwendeten Chips erfolgt durch die Bundesdruckerei.
Zu den Pässen und Personalausweisen anderer Staaten liegen der Bundesregierung keine Erkenntnisse vor.

27. Wie viele Unternehmensausweise und Kundenkarten welcher Modelle und Firmen sind nach Kenntnis der Bundesregierung jeweils potentiell betroffen?

Zu 27.

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

28. Wie viele Kartenlesegeräte welcher Modelle sind nach Kenntnis der Bundesregierung jeweils potentiell betroffen?

Zu 28.

Die Bundesregierung hat keine Kenntnis über das Kartenlesegeräte-Portfolio des betroffenen Anbieters. Vom BSI-zertifizierte Geräte sind nicht betroffen. Im Übrigen ist der Markt für derartige Geräte nicht reguliert.

29. Welche SIM-Karten sind nach Kenntnis der Bundesregierung überhaupt noch als sicher anzusehen (Bitte begründen)?

Zu 29.

Telekommunikationstechnik bietet keine absolute Sicherheit. Das gilt auch für SIM-Karten.

30. Hält die Bundesregierung einen Austausch der potentiell betroffenen Karten oder ein Offline-Update aus Sicherheitsgründen für notwendig und wenn ja
a) Was hat sie diesbezüglich bereits unternommen oder wird sie diesbezüglich wann unternehmen?
b) Welche Reaktionen, Aktivitäten und Ankündigungen seitens der betroffenen Hersteller, Telekommunikationsfirmen, Banken, Versicherungen etc. gab es bisher?
c) Welche Kosten entstünden nach Kenntnis der Bundesregierung durch den Austausch oder das Offline-Update der betroffenen Karten und wer wird diese Kosten tragen?
d) Wann und auf welchem Weg wird der Austausch vorgenommen und wie wird bis dahin verfahren?
e) Wie könnte ein Offline-Update an einem gesicherten Karten-Terminal technisch und praktisch durchgeführt werden und böte es dieselbe Sicherheit wie ein Vollaustausch der betroffenen Karten (Bitte begründen)?

Zu 30.

Nach Kenntnis der Bundesregierung ist die eGK nicht betroffen. Ein Austausch oder Update dieser Karten ist somit nicht angezeigt.
Im Falle von Debit- und Kreditkarten, die von Instituten ausgegeben werden, liegt die risikoorientierte Entscheidung über einen etwaigen Austausch von Karten bei den betroffenen Instituten.

Zur konkreten Machbarkeit eines entsprechend zeitnahen Austauschs oder Updates liegen keine Erkenntnisse vor, außer dass im Jahr 2010 das Einspielen eines Software-Updates auf mehrere Millionen Gemalto-Chipkarten über die Geldautomaten möglich war. Inwiefern dieser Mechanismus geeignet ist, für die Ausgabe kryptographischer Schlüssel verwendet zu werden, ist gegenwärtig unklar.

31. Wie wird sichergestellt, dass neu ausgegebene Karten nicht kompromittiert sind?

Zu 31.

Die Gematik hat in ihrer Stellungnahme vom 25. Februar 2015 bestätigt, dass die Produktion der Gesundheitskarten sehr hohen Sicherheitsstandards unterliegt, deren Einhaltung regelmäßig von Sicherheitsgutachtern geprüft wird. Im Übrigen wird auf die Antwort zu Frage 30 verwiesen.

32. Wäre nach Auffassung der Bundesregierung auch ein Online-Update möglich (bitte begründen) und wenn ja
a) In welchen Fällen?
b) Wie könnte sichergestellt werden, dass niemand den entsprechenden Datenverkehr mitspeichert und so auch die neuen Schlüssel abgreifen kann?

Zu 32.

Zur eGK wird auf die Antwort zu Frage 24, im Übrigen auf die Antwort zu Frage 30 verwiesen.

33. Wie viele Fälle von Angriffen durch ausländische Sicherheitsbehörden und Nachrichtendienste auf Trust Center und IT-Sicherheitsfirmen sind der Bundesregierung bekannt? (Bitte auflisten nach Jahr, Sicherheitsfirma, vermutlichem Angreifer und entstandenem Schaden)

Zu 33.

Der Bundesregierung liegen keine über die Medienberichterstattung hinausgehenden Erkenntnisse über Angriffe von ausländischen Sicherheitsbehörden auf nationale Trust Center und IT-Sicherheitsfirmen vor.

34. Hält die Bundesregierung andere europäische Verschlüsselungsstandards für notwendig und wenn ja, wann und in welcher Form wird sie sich dafür einsetzen? Wenn nein, warum nicht?

Zu 34.

Das BSI veröffentlich regelmäßig „Technische Richtlinien". In diesen Richtlinien werden u.a. Verschlüsselungs-Algorithmen empfohlen, die gegenwärtig als sicher gelten.

35. Gibt es nach Kenntnis der Bundesregierung bereits eine Reaktion der Internationalen Fernmeldeunion (ITU) und wenn ja, wie sah diese aus?

Zu 35.

Der Bundesregierung ist gegenwärtig keine Reaktion der Internationalen Fernmeldeunion (ITU) zu diesem Vorgang bekannt.

36. Gibt es nach Kenntnis der Bundesregierung bereits Reaktionen von Regulierungsbehörden oder den rund 800 Handy-Anbietern die der Mobilfunkverband GSMA weltweit vertritt und wenn ja wie sahen diese jeweils konkret aus?

Zu 36.

Der Bundesregierung sind gegenwärtig keine Reaktionen von Regulierungsbehörden oder dem Mobilfunkverband GSMA zu diesem Vorgang bekannt.

37. Könnten nach Einschätzung der Bundesregierung die von den Geheimdiensten erlangten Informationen dazu verwendet werden, um zukünftig die elektronische Gesundheitskarte und die dahinterstehende Telematik-Infrastruktur zu kompromittieren und die sensibelsten und schützenswertesten Daten der Versicherten einzusehen und zu missbrauchen? (Bitte begründen)

Zu 37.

Auf die Antwort zu Frage 24 wird verwiesen.

38. Kann die Bundesregierung die Behauptung der Gematik, elektronische Gesundheitskarten (eGK) seien nicht betroffen, weil sie auf anderen Produktionssystemen hergestellt würden und ein gleichzeitiger Angriff auf beide Produktionssysteme nach derzeitiger Erkenntnis auszuschließen sei (http://www.heise.de/newsticker/meldung/Gematik-Gesundheitskarten-sind-sicher-2560040.html), bestätigen?

Zu 38.
Auf die Antwort zu Frage 25 wird verwiesen.

39. Wie können nach Einschätzung der Bundesregierung solche Äußerungen erfolgen, wo doch auch der nun bekannt gewordene Angriff auf Gemalto nur durch die Veröffentlichungen einiger Snowden-Dokumente an die Öffentlichkeit kam?

Zu 39.
Die elektronische Gesundheitskarte verwendet andere technische und organisatorische Sicherheitskonzepte als die hier betroffenen SIM-Karten.

noch weitere Angriffe auf die Herstellungs- und Verarbeitungsprozesse der eGK – sei es durch die NSA, GCHQ oder aber auch durch andere – erfolgt sind oder zukünftig erfolgen?

Zu 40.
Cyber-Angriffe gegen informationstechnische Einrichtungen können nicht ausgeschlossen werden. Die Konzepte der Gematik für die Telematikinfrastruktur enthalten gerade vor dem Hintergrund möglicher Angriffe und Gefährdungen spezifische Sicherheitsvorkehrungen nach dem jeweils aktuellen Erkenntnisstand.
Das BSI unterstützt dabei die Gematik.

41. Teilt die Bundesregierung die Auffassung, dass die Stammdaten der Versicherten besonders schützenswerte Daten darstellen, sodass es nicht hinzunehmen wäre, wenn Stammdaten (Namen, Anschrift, Geburtsdatum und Versichertennummer) in die Hände Unbefugter gelangen würden? Wenn ja, welche Maßnahmen zum Schutz der Versicherten-Stammdaten hat sie bereits ergriffen, bzw. wird sie in die Wege leiten? Wenn nein, warum nicht?

Zu 41.

Die vier in der Frage genannten persönlichen Angaben dienen bei Vorlage der Karte unter anderem der Identifikation der Person, die die Karte beispielsweise bei einem Leistungserbringer vorlegt.

Bereits bei der in der Vergangenheit verwendeten Krankenversichertenkarte sowie der Europäischen Krankenversicherungskarte sind diese Daten entweder auf der Karte aufgedruckt bzw. können durch die dafür vorgesehenen Geräte etwa in Arztpraxen oder Krankenhäusern ausgelesen werden (die Anschrift ist nur elektronisch auslesbar). Eine Änderung hieran ist nach den Konzepten der Gematik für die eGK nicht vorgesehen.

Um im Übrigen die Karte auch als Europäische Krankenversicherungskarte nutzen zu können, ist der Aufdruck entsprechender Merkmale zudem auf EU-Ebene vereinbart worden.

42. Wie bewertet die Bundesregierung in diesem Zusammenhang die Aussagen der Betreiberfirma der elektronischen Gesundheitskarte Gematik, dass auch nach dem Hack bei Gemalto der Einsatz der eGK deshalb sicher sei, weil die Karten bisher keine medizinischen Daten beinhalten und auf dem Chip der eGK „lediglich die Stammdaten der Versicherten" gespeichert seien
(www.ihre-vorsor-ge.de/index.php?id=275&tx_ttnews%5Btt_news%5D=10583&cHash=34831bad107ff7d016777b15a4603b3d)?

43. Sieht die Bundesregierung, aufgrund der nun bekannt gewordenen wahrscheinlichen Kompromittierung von Gemalto-Sicherheits-Karten und der damit einhergehenden strukturellen Unsicherheit bei der Digitalisierung des Gesundheitswesens, eine Notwendigkeit ihren Gesetzentwurf für ein E-Health-Gesetz zurückzuziehen? (Bitte begründen)

44. Wird die Bundesregierung die gesetzlichen Voraussetzungen dafür schaffen, die dargestellten Sicherheitsmängel in der Digitalisierung des Gesundheitswesens zu korrigieren und wenn ja in welcher Form? (Bitte begründen)

45. Wird die Bundesregierung das Mammutprojekt eGK anlässlich der nach Auffassung der Fragesteller mit der Gemalto-Affäre deutlich werdenden mangelnden Technikfolgenabschätzung rückabwickeln? (Bitte begründen)

Zu 42. bis 45

Auf die Antwort zu Frage 24 wird verwiesen.

46. Wird die Bundesregierung eine patientenorientierte und datenschutzgerechte technische Infrastruktur im Gesundheitswesen schaffen und dafür sorgen, dass die durch die Snowden-Enthüllungen bekannt gewordenen illegalen Zugriffe ausländischer Geheimdienste auf Behörden, Firmen und Datenbestände in Deutschland untersucht und mit allen zur Verfügung stehenden legalen Mitteln unterbunden werden? Wenn ja, in welcher Form? Wenn nein, warum nicht?

Zu 46.

Die Schaffung einer patientenorientierten und datenschutzgerechten technischen Infrastruktur im Gesundheitswesen ist das Ziel der Einführung der Telematikinfrastruktur.

47. Welche dezentralen Konzepte, die ohne große Datenmengen an einem Ort, wie sie manche Anwendungen der eGK mit sich bringen, auskommen, sind der Bundesregierung als Alternativen zur eGK bekannt?

Zu 47.

Nach Auffassung der Bundesregierung ist die eGK in der Hand der Patientinnen und Patienten das geeignete Instrument, um den behandelnden Personen bei Bedarf Daten sicher und verlässlich zur Verfügung stellen können.