

Kleine Anfrage

der Abgeordneten Jan Korte, Ulla Jelpke, Katja Kipping, Petra Pau, Frank Tempel, Kathrin Vogler, Halina Wawzyiak und der Fraktion DIE LINKE.

Konsequenzen nach Angriff auf weltweit größten Chipkartenhersteller durch die Geheimdienste NSA und GCHQ

Bei dem Versuch, die weltweite Kommunikation überwachen und kontrollieren zu können, geraten zunehmend Internetsicherheitsfirmen 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 Hackerspezialeinheit des britischen Geheimdienstes Government Communications Headquarters (GCHQ) und des US-amerikanischen Geheimdienstes National Security Agency (NSA) die Verschlüsselungscodes für SIM-Karten des niederländischen Chip- und Magnetstreifenkartenherstellers Gemalto erbeutet haben soll (<https://firstlook.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 Handykommunikation 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 Cyberangriffe 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 Mobilfunkkunden 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 Geheimdienstaktion eingeschätzt wird. Giesecke & Devrient erklärte hingegen, dass die Firma „bisher keine Erkenntnisse darüber, dass SIM-Karten-Schlüssel entwendet wurden“ habe (vgl. SPIEGEL ONLINE vom 25. Februar 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 (OTA – 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 Angriffsszenarien werden ebenfalls in einem der Snowden-Dokumente als mögliches Ziel erwähnt (vgl. ZEIT ONLINE vom 25. Februar 2015).

Durch das Kompromittieren des Gemalto-Firmennetzes könnten darüber hinaus insbesondere auch für das IT-Großprojekt elektronische Gesundheitskarte (eGK) neue und massive Sicherheitsgefahren entstanden sein. So lieferte allein Gemalto in den vergangenen Jahren für die AOK, Deutschlands größte 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 Dr. 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-gesundheits-nachrichten.de/2015/02/26/e-card-angst-vor-datenmissbrauch-ueberschattet-medizinischen-nutzen/).

Wir fragen die Bundesregierung:

1. Welche Erkenntnisse hat die Bundesregierung seit welchem Zeitpunkt über den geheimdienstlichen Angriff auf den niederländischen Chip- und Magnetstreifenkartenhersteller Gemalto?
2. Welche Erkenntnisse hat die Bundesregierung seit welchem Zeitpunkt über einen möglichen geheimdienstlichen Angriff auf den deutschen SIM-Kartenhersteller Giesecke & Devrient?
3. Revidiert die Bundesregierung nach Bekanntwerden des Gemalto-Hacks ihre Position, dass kein US-amerikanischer Geheimdienst deutsche Unternehmen und Konzerne ausspäht (vgl. die Antwort der Bundesregierung zu Frage 5 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2281)?

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?
5. Revidiert die Bundesregierung nach Bekanntwerden des Gemalto-Hacks ihre Antwort zu Frage 8 der Kleinen Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 18/2281), wonach sie keine Erkenntnisse zu Wirtschaftsspionage durch die NSA oder andere US-Dienste in anderen Staaten habe, und wenn ja, in welcher Form?
Wenn nein, warum nicht?
6. Wie schätzt die Bundesregierung die durch den Gemalto-Hack und mögliche weitere Angriffe befreundeter Geheimdienste auf IT-Sicherheitsunternehmen bestehende Bedrohungslage ein?
7. Teilt die Bundesregierung die Einschätzung von Prof. Dr. Hartmut 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?
8. Hält die Bundesregierung neben der Überwachungsproblematik auch Identitätsdiebstahl, also das Täuschen mit falschen Identifizierungsnachweisen, als Folge des Gemalto-Hacks für möglich (bitte begründen)?
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?
10. Welche Maßnahmen haben Bundesregierung und deutsche Sicherheitsbehörden infolge des geheimdienstlichen Angriffs von NSA und GCHQ auf den niederländischen SIM-Kartenhersteller Gemalto wann in die Wege geleitet, und welche Ergebnisse hatten diese jeweils?
11. Welche Sicherheitsbehörden oder staatlichen Stellen erfassen in welcher Form und aufgrund welcher Informationen und Meldewege die Häufigkeiten, Schwere und Konsequenzen von Cyberangriffen statistisch, und wird dabei auch nach Angriffen durch Geheimdienste oder andere Cyberkriminelle differenziert?
12. Was wurde nach Kenntnis der Bundesregierung von wem unternommen, um auszuschließen, dass Geräte noch „infiziert“ sind?
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?
14. Wie charakterisiert die Bundesregierung geheimdienstliche Angriffe auf Chipkartenhersteller, und hält sie eine strafrechtliche Verfolgung für geboten (bitte begründen)?

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?
16. Hat sich die Bundesregierung infolge 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?
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)?
18. Welche Chip- und Magnetstreifenkartenprodukte sind nach Kenntnis der Bundesregierung potenziell von dem Gemalto-Hack durch NSA und GCHQ betroffen?
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?
20. Welcher wirtschaftliche Schaden ist nach Erkenntnissen der Bundesregierung schätzungsweise dadurch entstanden?
21. Welche Bundesministerien, Bundesbehörden und sicherheitsrelevanten Einrichtungen und Bereiche in der Bundesrepublik Deutschland sind potenziell durch den Krypto-Schlüsseldiebstahl in jeweils welchem Ausmaß betroffen?
22. Wie viele SIM-Karten welcher Modelle und welcher Telefongesellschaften und Telekommunikationsanbieter sind nach Kenntnis der Bundesregierung potenziell betroffen?
23. Wie viele EC- bzw. Kreditkarten welcher Modelle und welcher Banken sind nach Kenntnis der Bundesregierung potenziell betroffen?
24. Wie viele eGK-Karten welcher Modelle und welcher Krankenversicherungen sind nach Kenntnis der Bundesregierung potenziell betroffen?
25. Kann die Bundesregierung die Pressemeldung der Gematik vom 25. Februar 2015 bestätigen (www.e-health-com.eu/details-news/gematik-veroeffentlicht-stellungnahme-zum-versuchten-angriff-auf-kartenherstellergemalto/b93cf7591c081503b74de1d4e40c5798/) und definitiv ausschließen, dass von dem Angriff der Geheimdienste der USA und Großbritanniens auf den Kartenhersteller Gemalto elektronische Gesundheitskarten betroffen sind?
26. Wie viele Pässe und Personalausweise welcher Staaten sind nach Kenntnis der Bundesregierung jeweils potenziell betroffen?
27. Wie viele Unternehmensausweise und Kundenkarten welcher Modelle und Firmen sind nach Kenntnis der Bundesregierung jeweils potenziell betroffen?
28. Wie viele Kartenlesegeräte welcher Modelle sind nach Kenntnis der Bundesregierung jeweils potenziell betroffen?

29. Welche SIM-Karten sind nach Kenntnis der Bundesregierung überhaupt noch als sicher anzusehen (bitte begründen)
30. Hält die Bundesregierung einen Austausch der potenziell 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 Kartenterminal technisch und praktisch durchgeführt werden, und böte es dieselbe Sicherheit wie ein Vollaustausch der betroffenen Karten (bitte begründen)?
31. Wie wird sichergestellt, dass neu ausgegebene Karten nicht kompromittiert sind?
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?
33. Wie viele Fälle von Angriffen durch ausländische Sicherheitsbehörden und Nachrichtendienste auf Trust Center und IT-Sicherheitsfirmen sind der Bundesregierung bekannt (bitte nach Jahr, Sicherheitsfirma, vermutlichem Angreifer und entstandenem Schaden auflisten)?
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?
35. Gibt es nach Kenntnis der Bundesregierung bereits eine Reaktion der Internationalen Fernmeldeunion (ITU), und wenn ja, wie sah diese aus?
36. Gibt es nach Kenntnis der Bundesregierung bereits Reaktionen von Regulierungsbehörden oder den rund 800 Handybietern die der Mobilfunkverband GSMA weltweit vertritt, und wenn ja, wie sahen diese jeweils konkret aus?
37. Könnten nach Einschätzung der Bundesregierung die von den Geheimdiensten erlangten Informationen dazu verwendet werden, um zukünftig die elektronische Gesundheitskarte und die dahinterstehende Telematikinfrastruktur zu kompromittieren und die sensibelsten und schützenswertesten Daten der Versicherten einzusehen und zu missbrauchen (bitte begründen)?
38. Kann die Bundesregierung die Behauptung der Gematik, elektronische Gesundheitskarten seien nicht betroffen, weil sie auf anderen Produktionssystemen hergestellt würden und ein gleichzeitiger Angriff auf beide Produktionssysteme nach derzeitiger Erkenntnis auszuschließen sei (www.

heise.de/newsticker/meldung/Gematik-Gesundheitskarten-sind-sicher-2560040.html), bestätigen?

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?
40. Mit welcher Wahrscheinlichkeit kann die Bundesregierung ausschließen, dass noch weitere Angriffe auf die Herstellungs- und Verarbeitungsprozesse der eGK – sei es durch NSA, GCHQ oder aber auch durch andere – erfolgt sind oder zukünftig erfolgen?
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 Versichertenstammdaten hat sie bereits ergriffen, bzw. wird sie in die Wege leiten?
Wenn nein, warum nicht?
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-vorsorge.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-Sicherheitskarten und der damit einhergehenden strukturellen Unsicherheit bei der Digitalisierung im Gesundheitswesen 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 im Gesundheitswesen 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)?
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?
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?

Berlin, den 26. März 2015

Dr. Gregor Gysi und Fraktion

