

dieDatenschützer Rhein Main

- keine Untaten mit Bürgerdaten -

E-Mail: kontakt@ddrm.de Internet: <http://ddrm.de/>

Frankfurt, den **24.02. 2015**

Bundesministerium für Gesundheit
Herrn Bundesminister Hermann Gröhe
Rochusstr. 1

53123 Bonn

Nach dem erfolgreichen Angriff der Geheimdienste NSA (USA) und GCHQ (Großbritannien) auf Chipkarten-Hersteller Gemalto das Projekt gematik / elektronische Gesundheitskarte einstellen und E-Health-Gesetzentwurf zurückziehen

Sehr geehrter Herr Bundesgesundheitsminister Gröhe,

die neuesten Veröffentlichungen aus den Dokumenten von Edward Snowden sind für uns Anlass, uns an Sie zu wenden.

Spätestens nach dem Nachweis, dass der Chipkarten-Hersteller Gemalto, der auch einen großen Teil der bisher eingesetzten elektronischen Gesundheitskarten (eGk) hergestellt hat, durch die Geheimdienste NSA und GCHQ erfolgreich angegriffen wurde wird deutlich: Es gibt keine Sicherheit für eine zentralisierte Speicherung von Gesundheitsdaten von Millionen Menschen. Gleiches gilt für technische Systeme, die einen zentralisierten Zugriff auf dezentral gespeicherte Daten zulassen. Wir fordern Sie daher auf,

- den von Ihnen veröffentlichten Gesetzentwurf für ein E-Health-Gesetz zurückzuziehen,
- die gesetzlichen Voraussetzungen dafür zu schaffen, die Fehlentwicklungen in der Digitalisierung des Gesundheitswesens zu korrigieren,
- das Mammutprojekt eGK anlässlich der mit der Gemalto-Affäre deutlich werdenden mangelnden Technikfolgenabschätzung rückabzuwickeln,
- eine patientenorientierte und datenschutzgerechte technische Infrastruktur im Gesundheitswesen zu schaffen und
- sich innerhalb der Bundesregierung dafür einzusetzen, dass die durch die Snowden-Enthüllungen bekannt gewordenen illegalen Zugriffe ausländischer Geheimdienste auf Behörden, Firmen und Datenbestände in Deutschland endlich untersucht und mit allen zur Verfügung stehenden legalen Mitteln unterbunden werden.

Den Geheimdiensten der USA und Großbritanniens ist es - den jüngst veröffentlichten Snowden-Dokumenten zufolge - schon im Jahr 2010 gelungen, Sicherheitskonzepte des Chipkarten-Herstellers Gemalto zu überwinden und bis jetzt unbemerkt an deren Sicherheitsschlüssel zu gelangen. Dieses Unternehmen hat nicht nur SIM-Karten für Handys hergestellt, sondern auch die elektronischen Gesundheitskarten für 25 Millionen AOK-Versicherte sowie Kartenlesegeräte für Arztpraxen hergestellt und ausgeliefert. Wenn dieses Datenleck dem Unternehmen nicht aufgefallen ist muss vermutet werden, dass interne Kontrollen völlig versagt haben müssen. Allein die potenziellen Auswirkungen dieser Entwicklung auf die gesamte telematische Infrastruktur erfordern einen sofortigen Stopp dieses Projekts.

Paul Beverly, ein Vizepräsident von Gemalto, gibt sich laut The Intercept *“verstört und beunruhigt”* (Zitat: *„Beverly said, ‚I am totally unaware. To the best of my knowledge, no.’”* – Quelle: <https://firstlook.org/theintercept/2015/02/19/great-sim-heist/>). Wir alle haben Anlass, verstört und beunruhigt zu sein; Sie auch, sehr geehrter Herr Bundesgesundheitsminister!

Professor Hartmut Pohl, Mitglied des Beirats der International Security Academy und Sprecher des Arbeitskreises Datenschutz und IT-Sicherheit der Gesellschaft für Informatik e. V., erklärte: *“Dies ist nicht das erste Mal, dass ein Trust Center von Sicherheitsbehörden und Nachrichtendiensten wie der NSA geknackt wurde und alle Schlüssel ausgelesen werden konnten. Die erfolgreichen Angriffstechniken funktionieren auch für SIM-Karten und Handy-Schlüssel. Dies sind über 5 Jahre alte Angriffe. Bei softScheck gehen wir davon aus, dass aktuell weltweit praktisch kein Server angriffssicher ist. In Deutschland dürften aktuell weit über 50.000 der wichtigsten Server in Unternehmen, Regierung und Verwaltung mit Backdoors der NSA versehen sein (‚Strategic Servers’)...”* (Quelle: <http://www.stoppt-die-e-card.de/index.php?/archives/299-Chipkarten-Hack-und-die-Folgen-Kommentare-der-Experten-2,0.html>).

Es ist für Sie also Zeit zum Handeln, um sensibelste Gesundheitsdaten von Millionen Menschen vor illegalen Zugriffen zu schützen und Fehlentwicklungen in der Gesundheitspolitik der Vergangenheit zu korrigieren!

Mit freundlichen Grüßen

dieDatenschützer Rhein Main

<http://ddrm.de/>

gez. Uli Breuer, Roland Schäfer, Walter Schmidt

dieDatenschützer Rhein Main (<http://ddrm.de/>) sind

eine Gruppe des Arbeitskreis Vorratsdatenspeicherung (<http://vorratsdatenspeicherung.de/>),

Partner der Aktion: Stoppt die e-Card! (<http://www.stoppt-die-e-card.de/>) und

Partner des Bündnis „Demokratie statt Überwachung“ (<https://www.demokratie-statt-ueberwachung.de/>).

Hervorgegangen ist die Gruppe aus der Volkszählungsbewegung „11gegenZensus11“. Die aktuellen Arbeitsschwerpunkte sind ein unabhängiges Frankfurter Datenschutzbüro, die Videoüberwachung des öffentlichen Raums und von politischer Aktivitäten (Demonstrationen und Kundgebungen), die Elektronische Gesundheitskarte, die Vorratsdatenspeicherung sowie weitere Datenschutzthemen.

Per E-Mail: : kontakt@ddrm.de

Spendenkonto:

PSD Bank Hessen-Thüringen eG Kontonummer: 514 819 7000 / BLZ: 500 909 00

IBAN: DE77 5009 0900 5148 1970 00 / BIC: GENODEF1P06