4218/J XXV. GP

Eingelangt am 19.03.2015

ANFRAGE

der Abgeordneten MMMag. Dr. Kassegger, Kunasek
und weiterer Abgeordneter
an den Bundesminister für Landesverteidigung und Sport
betreffend Gemalto-Hack

Glaubt man einem Bericht des Standards vom 25.2.2015[1], dann haben NSA und GCHQ schon vor Jahren beim Sim- Karten Hersteller Gemalto *„Computersysteme des Unternehmens gehackt und dabei unter anderem jene Schlüssel gestohlen, die eigentlich Mobilfunknetze gegen unbeschränktes Abhören sichern sollen."*

Nicht nur SIM-Karten zum Telefonieren sind betroffen. Es sind Bankomatkarten, Reisepässe, Personalausweise und möglicher Weise auch Technologien aus dem NFC- (*Near Field Communication*) und RFID-Bereich (*Radio-frequency identification*) ebenso betroffen, wie RadioFM4 online berichtet. Nach diesem Onlinebericht von RadioFM4[2] vom 23 02 2015 sind möglicher Weise auch Bereiche aus „Industrie 4.0" wie Verkehrs- und Industrievernetzung, Maschinenkommunikation, Telematikdaten aus Fahrzeugen, Smart Meter für Strom, Gas und Wassernetze, sowie Steueranlagen von Wohnungen und Hausleitsystem, sowie Sensornetze gefährdet. RadioFM4 zur Authentifizierung: *„Der eigentliche Grund, warum die Netzneutralität EU-weit in Frage steht, soll ein eigener, privilegierter Kommunikationskanal in alle Mobilfunknetze sein. Die Authentifizierung der vernetzten Sensoren und Steuerungselemente und die Verschlüsselung des Datenverkehrs aber soll über SIM-Cards erfolgen"*
Die neu vorgestellten Generationen von universellen SIM-Karten und Safe-Cards sollen bereits einen Mini-PC enthalten, der über das Internetprotokoll verschlüsselt kommunizieren kann und völlig fernadministrierbar ist.

Unter Zugrundelegung des Rahmenvertrages der Bundesbeschaffungsgesellschaft m.b.H. (BBG) ist der Anbieter für Mobiltelefone des Verteidigungsministeriums A1. Im

[1] http://derstandard.at/2000012136548/Gemalto-Wurden-gehackt-SIM-Karten-aber-nicht-gefaehrdet

[2] http://fm4.orf.at/stories/1754449/

[3] http://www.miles.ac.at/miles/sites/Services/IT_Service.php?pers=hlo

Jahresdurchschnitt werden **beim Bundesheer 4.300 A1-Mobiltelefone** und somit auch **4.300 SIM-Cards** verwendet.

Beim Österreichischen Bundesheer ist aber auch die verschlüsselte 3.VE[3] (3. Verarbeitungsebene) im Einsatz. Diese 3.VE dient sowohl der Bundesheerverwaltung, wird aber auch für den Einsatz und in den verschiedenen Sicherheitsstufen des Bundesheeres verwendet. Im Rahmen der aktuellen Umstellung von Windows XP auf Windows7 werden über **20.000 Safe-Cards** der 3.VE getauscht und neu eingeführt. Diese Safe-Cards sind in Zusammenhang mit einem Passwort der Zugangsschlüssel zum verschlüsselten EDV-Netzwerk des Bundesheeres.

In diesem Zusammenhang richten die unterfertigten Abgeordneten an den Bundesminister für Landesverteidigung und Sport nachstehende

ANFRAGE

1) Stammen die 20.000 neuen Safe-Cards für die verschlüsselten 3.VE EDV-Arbeitsplätze des Bundesheeres von der Firma GEMALTO?

2) Wenn nein, von welcher anderen Firma stammen sie?

3) Wenn ja, werden die Safe-Cards ausgetauscht?

4) Ist sichergestellt, dass diese Safe- Cards dieser Firma nicht von einem möglichen Hackerangriff betroffen waren?

5) Sind die beim Bundesheer nun neu einzuführenden Safe-Cards mit einem Betriebssystem ausgestattet und bieten sie die Möglichkeit verschlüsselt zu kommunizieren bzw. sind sie fernadministrierbar?

6) Sind die beim Bundesheer verwendeten 4.300 Diensttelefone mit SIM-Cards der Firma GEMALTO oder einer anderen vom Hackangriff betroffenen Firma ausgestattet?

7) Welche sicherheitstechnischen Maßnahmen werden Sie in Absprache mit ihrem Informationssicherheitsbeauftragten des BMLVS ergreifen um die Sicherheit im Bereich der Diensttelefone und der 3.VE sicher zu stellen und die Gefahr eines Smart-Card-Hackings oder SIM-Card-Hackings auf Grund der aktuellen möglichen Sicherheitsbedrohung durch den GEMALTO-Hack in ihrem Verantwortungsbereich abzuwehren?