

02.04.2015

Antwort

der Landesregierung

auf die Kleine Anfrage 3180 vom 2. März 2015
des Abgeordneten Daniel Schwerd PIRATEN
Drucksache 16/8039

Der Chipkarten-Angriff: Wird die Integrität kritischer elektronischer Infrastruktur durch westliche Geheimdienste verletzt?

Der Minister für Inneres und Kommunales hat die Kleine Anfrage 3180 mit Schreiben vom 1. April 2015 namens der Landesregierung im Einvernehmen mit der Ministerpräsidentin und allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

*„Alles Reden ist sinnlos, wenn das Vertrauen fehlt.“
Franz Kafka*

Am 19. Februar 2015 berichtete das investigative Internetmagazin „The Intercept“ über der Öffentlichkeit bislang unbekannt, intern als „top secret“ klassifizierte Dokumente des britischen Geheimdienstes GCHQ, die den Journalisten durch Edward Snowden zur Verfügung gestellt worden sind. Den Unterlagen zufolge hat der britische Geheimdienst das niederländische Unternehmen Gemalto kompromittiert und sich Sicherheitsschlüssel der dort produzierten Chips und SIM-Karten beschafft. Gemalto ist der weltgrößte Hersteller von Chip-Karten, er beliefert u.a. sämtliche Mobiltelefonanbieter Deutschlands. Neben SIM-Karten sind allerdings auch elektronische Gesundheitskarten von Krankenkassen sowie Kreditkarten betroffen. Mit den erbeuteten Schlüsseln ist es möglich, verschlüsselte Kommunikation zu entschlüsseln und die digitale Authentifizierung zu fälschen, die auf Basis dieser Chip-Karten realisiert wird.

Gemalto hat den Einbruch in seine Infrastruktur bestätigt. Ebenso bestätigt hat es den Diebstahl von Schlüsseln, die zu 2G-SIM-Karten gehören. Das Risiko für 3G-SIM-Karten hält Gemalto selbst für gering, da hier eine zusätzliche Sequenznummer Teil der Verschlüsse-

Datum des Originals: 01.04.2015/Ausgegeben: 09.04.2015

Die Veröffentlichungen des Landtags Nordrhein-Westfalen sind einzeln gegen eine Schutzgebühr beim Archiv des Landtags Nordrhein-Westfalen, 40002 Düsseldorf, Postfach 10 11 43, Telefon (0211) 884 - 2439, zu beziehen. Der kostenfreie Abruf ist auch möglich über das Internet-Angebot des Landtags Nordrhein-Westfalen unter www.landtag.nrw.de

lung ist. Experten wiederum halten den Schutz durch die zusätzliche Sequenznummer für nicht ausreichend.¹

Die Deutsche Telekom hat mittlerweile erklärt, die Schlüssel der von Gemalto bezogenen SIM-Karten zu verändern zu wollen. Darüber hinaus sehe die Deutsche Telekom keinen weiteren Handlungsbedarf, betont aber gleichzeitig, die Kompromittierung ihres Schutzmechanismus nicht vollkommen ausschließen zu können.²

Zu dem Problem des so genannten „Over-the-Air“-Angriffs mit stillen System-SMS, bei dem etwa die Aktualisierung der SIM-Karte von Dritten „gehackt“ oder Malware heimlich aufgeladen werden kann, haben sich weder die Telekom noch Gemalto geäußert.

Die teilweise widersprüchlichen Informationen und fehlenden Antworten geben bei Anwendung allgemeiner Sorgfaltspflichten keinen Grund zur Entwarnung.

- 1. Nutzen die Landesregierung, Landesbehörden, Ministerien bzw. landeseigene Betriebe Chips des Herstellers Gemalto für Mobiltelefone, den BOS Digitalfunk oder andere Anwendungen? Schlüsseln Sie die Angaben nach betroffenen Stellen auf und nennen die jeweilige Anzahl betroffener Chip-Karten.**
- 2. Sieht die Landesregierung die Sicherheit der Kommunikation und Authentifikation auf Basis von Chipkarten des Herstellers Gemalto noch als ausreichend integer an? Begründen Sie Ihre Ansicht.**

Hinsichtlich der eingesetzten Mobiltelefone ist eine vollständige Abfrage mit der gefragten Zielsetzung im Rahmen der für die Beantwortung einer Kleinen Anfrage vorgesehenen Zeit nicht leistbar. Die Landesverwaltung nutzt Mobilfunk- und vergleichbare Karten in großer Zahl. Die Vertragspartner der Landesverwaltung setzen im Bereich des Mobilfunks u.a. Karten der Firma GEMALTO ein. Auf Nachfrage der Landesregierung haben maßgebliche Vertragspartner geantwortet, dass auch ihnen eine Identifizierung der potentiell betroffenen Karten nicht ohne weiteres möglich ist.

Beim BOS-Digitalfunk werden die Sicherheitskarten als Rohlinge ohne jede Software von T-Systems geliefert. Die erforderliche Software wird durch das BSI unter strenger Beachtung der Sicherheitsvorschriften aufgebracht und danach mit dem derzeit gültigen Schlüssel für das BOS-Digitalfunknetz versehen. Somit ist eine Kompromittierung des Schutzmechanismus des Herstellers in der dargestellten Form hier nicht möglich.

Bei weiteren Anwendungen, wie z.B. in der Finanzverwaltung, werden zurzeit ca. 4.500 Chip-Karten für die verwaltungsinterne Mailverschlüsselung und für Telearbeit eingesetzt. Die Zertifikate werden vom Rechenzentrum der Finanzverwaltung NRW verwaltet und über einen Rahmenvertrag von IT.NRW bezogen. Bei IT.NRW sind zur Telearbeit etwa 6.200 Chipkarten im Einsatz. IT.NRW erstellt die Zertifikate für die Telearbeit und Chipkarten mit DOI-Zertifikaten selbst und bringt diese auf die Karten auf, so dass das Angriffsszenario hier keine Auswirkung gehabt hätte.

¹ <http://www.heise.de/newsticker/meldung/SIM-Karten-Affaere-Auch-3G-Netze-nicht-vor-Spionage-sicher-2560250.html>

² <https://telekomhilft.telekom.de/t5/Blog/SIM-Karten-des-Herstellers-Gemalto/ba-p/1293033>

Für die elektronischen Gesundheitskarten (eGK) stellt GEMALTO auch Prozessorkarten (insbesondere Kryptochipkarten) her. Auf Anfrage der gematik GmbH, die gemäß § 291 a SGB V in Deutschland für den Betrieb und die Sicherheit der eGK zuständig ist, hat GEMALTO mitgeteilt, dass die Produktionssysteme für die eGK nach derzeitigem Erkenntnisstand nicht von evtl. Angriffen betroffen waren.

Nach Auskunft maßgeblicher Vertragspartner der Landesverwaltung setzen diese standardmäßig eine zusätzliche Verschlüsselungsebene ein und sehen daher keinen weiteren Handlungsbedarf. Darüber hinaus bestreitet der Hersteller GEMALTO in seiner Pressemitteilung die Entwendung der Schlüssel.

3. Welche Maßnahmen ergreift die Landesregierung, um sich selbst, die Kommunen, Bürger und Unternehmen dieses Landes vor dem Ausspähen mithilfe der entwendeten Schlüssel von Chipkarten des Herstellers Gemalto zu schützen?

Der Landesregierung liegen keine Erkenntnisse darüber vor, dass sich kompromittierte Karten in Verwendung durch die Landesverwaltung, die Kommunen, die Bürger oder Unternehmen befinden.

Zu den grundsätzlichen Maßnahmen der Landesregierung mit Bezug zur Informationssicherheit wurde bereits ausführlich in der Antwort zur Kleinen Anfrage 3097 (LT.-Drs. 16/8029) in der Antwort zu Frage 2 Stellung genommen.

4. An wen können sich Bürger, Unternehmen und Kommunen des Landes NRW wenden, um die Sicherheit ihrer SIM- und Chipkarten zu überprüfen?

Im Zweifel ist der jeweilige Vertragsanbieter durch den Vertragsnehmer zu kontaktieren.

5. Wie bewertet die Landesregierung den Verlust der Vertraulichkeit und Integrität elektronischer Kommunikation in Bereichen der kritischen Infrastrukturen wie Finanzwesen, Gesundheitswesen und Telekommunikation?

In diesem konkreten Fall ist ein Verlust der Vertraulichkeit und Integrität zurzeit nicht festzustellen.

Die Landesregierung nimmt die Sicherheitsbedrohung sehr ernst. Deswegen werden seit vielen Jahren in der Landesverwaltung organisatorische und praktische Maßnahmen zur Informationssicherheit umgesetzt und diese nach Stand der Technik weiterentwickelt.

Es ist aber festzustellen, dass eine absolute Sicherheit jetzt und in Zukunft nicht erreicht werden kann. Die Landesverwaltung kommuniziert intern bereits seit vielen Jahren vorrangig innerhalb interner Netze (LVN, CN-Pol, Netz der Finanzverwaltung). Im Übrigen findet Kommunikation mit dem Bürger oder Unternehmen von Landesseite aus typischerweise nicht über Mobilfunk statt.