



Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Herrn
Jan Korte, MdB
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)

FAX +49 (0)

INTERNET www.bmi.bund.de

DATUM 9. September 2013

BETREFF **Schriftliche Frage Monat September 2013**
HIER **Arbeitsnummer 8/412**

ANLAGE - 1 -

Sehr geehrter Herr Abgeordneter,

auf die mir zur Beantwortung zugewiesene schriftliche Frage übersende ich Ihnen die beigefügte Antwort.

Mit freundlichen Grüßen
in Vertretung

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

VERKEHRSANBINDUNG S-Bahnhof Bellevue, U-Bahnhof Turmstraße

Bushaltestelle Kleiner Tiergarten

Schriftliche Frage des Abgeordneten Jan Korte
vom 30. August 2013
(Monat August 2013, Arbeits-Nr. 8/412)

Frage

Wie hoch sind die bislang angefallenen und geschätzten Gesamtkosten für das Projekt neuer Personalausweis (bitte aufschlüsseln nach Planung, Entwicklung, Sicherheit, Einführung, künftig anzubietende online-Dienste im Rahmen von E-Government einschließlich: Berechtigungszertifikate, ID-Service, IT-System-, Software- und IT-Integrationskosten), und welche Konsequenzen wird die Bundesregierung nach dem erneuten Hack eines neuen Personalausweises durch den Chaos Computer Club und den dadurch aufgezeigten Sicherheitsproblemen (vgl. Sendung von report München vom 27. August 2013) ziehen (bitte begründen)?

Antwort

Das Bundesministerium des Innern (BMI) ist vom Rechnungsprüfungsausschuss des Deutschen Bundestages aufgefordert, bis zum 30. Dezember 2013 über die Ausgaben des neuen Personalausweises zu informieren. Insoweit wird auf den Bericht verwiesen.

Im Vorgriff auf den anstehenden Bericht beziffert das BMI die Gesamtausgaben bis zum Abschluss des Projekts „Einführung neuer Personalausweis“, also bis Ende 2011 im Bereich BMI, Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesverwaltungsamt (BVA) auf insgesamt 16,6 Mio. €. Diese Ausgaben entstanden im Wesentlichen im Zuge der Beauftragung von Unternehmen durch BMI, BSI und BVA.

Darüber hinaus hat die Bundesregierung im Rahmen des IT-Investitionsprogramms (als Teil des Investitions- und Tilgungsfonds) in den Jahren 2009 und 2010 Mittel in Höhe von 41 Mio. € für Maßnahmen zur Beförderung der Online-Ausweisfunktion bereitgestellt (insbesondere Durchführung eines Anwendungstests, Förderung von Kartenlesern, Bereitstellung einer Software zur Nutzung der Online-Ausweisfunktion, Service-Supportleistungen).

Außerhalb des BMI sind weitere Kosten bei den unterschiedlichsten Stellen entstanden, u. a. bei IT-Dienstleistern, eID-Servicebetreibern oder etwa auch bei Anbietern, die Online-Anwendungen für die Online-Ausweisfunktion geschaffen haben. Die Höhe der dort entstandenen Kosten ist der Bundesregierung nicht bekannt.

Die Kosten der Antragsbearbeitung in den Personalausweisbehörden und die Produktion des neuen Personalausweises beim Ausweishersteller werden über die Personalausweisgebühr finanziert.

Die Bundesregierung sieht keine Veranlassung, Konsequenzen aus den Darstellungen von Report München in der Sendung vom 27. August 2013 zu ziehen. Es trifft nicht zu, dass der Chip des neuen Personalausweises „gehackt“ wurde.

In den drei Jahren seit seiner Einführung gab es keinerlei Vorfälle, die Zweifel an der Sicherheit des Chips und der in ihm gespeicherten Daten hervorrufen. Der neue Personalausweis ist mit elektronischen Sicherheitsmerkmalen auf höchstem technologischem Niveau ausgestattet. Alle Informationen und Übertragungen werden mit modernen, dauerhaft wirksamen und international anerkannten Verschlüsselungsverfahren sicher geschützt. Ein Zugriffssystem, das auf staatlich vergebenen Berechtigungszertifikaten beruht, regelt, wer auf welche personenbezogenen Daten zugreifen darf.

In dem von Report München dargestellten Angriffsszenario ging es dagegen darum, dass ein privat verwendeter PC mit Schadsoftware, u. a. einem sog. Keylogger, infiziert wurde. Beim Einsatz des neuen Personalausweises an diesem infizierten PC mit einem Basislesegerät (also einem Lesegerät ohne eigenes Tastaturfeld) wurde die notwendige Geheimzahl (PIN) abgefangen, weil sie über die Tastatur bzw. über eine virtuelle Tastatur eingegeben wurde.

Vor einem solchen Szenario kann sich der Bürger durch regelmäßige Aktualisierung des Betriebssystems, ein aktuelles Virenschutzprogramm sowie eine Firewall schützen. Diese einfachen Vorsichtsmaßnahmen gelten als Basisschutz für jeden Computer. Informationen hierzu sind breitflächig verfügbar (z. B. Deutschland sicher im Netz, BSI für Bürger).

Darüber hinaus stellt allein die Kenntnis der PIN kein Sicherheitsrisiko dar. Die im Chip gespeicherten Daten können nämlich nur dann ausgelesen werden, wenn zugleich auch der Ausweis auf dem Kartenleser liegt („Besitz und „Wissen“, sog. Zwei-Faktor Authentifizierung).

Der Ausweis kann also bei Kenntnis der PIN nur missbraucht werden, wenn er selbst zur Verfügung steht (z. B. gestohlen wird) und die eID noch nicht im Sperrregister gesperrt wurde.

Darüber hinaus wird darauf hingewiesen, dass auf dem Markt mittlerweile zahlreiche höherwertige Kartenleser mit eigener Tastatur angeboten werden, die das Abfangen der PIN selbst bei infiziertem Computer ausschließen.

Die Online-Ausweisfunktion ist sicher. Sie bietet wesentlich mehr Sicherheit gegenüber der bis heute verbreiteten Verwendung von „Benutzername und Passwort“. Sie schützt damit wirksam vor dem zunehmenden Identitätsdiebstahl im Internet.

Die Rente ist sicher!