



Murks bei IT-Großprojekten hat Methode

Rede von Jan Korte, 25. April 2013

Rede zu Protokoll zur:

Ersten Beratung des von der Koalition eingebrachten Gesetzentwurfs zur Änderung des Bundeszentralregistergesetzes und anderer registerrechtlicher Vorschriften zum Zweck der Zulassung der elektronischen Antragstellung bei Erteilung einer Registerauskunft (Drucksache 17/13222)

Sehr geehrter Herr Präsident,
werte Kolleginnen und Kollegen,

im Endspurt der Wahlperiode und bemüht um eine Aufbesserung ihrer miesen Bilanz, führt die Koalition auf ziemlich halsbrecherische Weise einige ihrer fragwürdigen oder sogar gescheiterten Großprojekte im Bereich der Informations- und Kommunikationstechnik (IKT) zusammen. Keine Rolle spielen dabei Gefahren für die Daten der Bürgerinnen und Bürger, klare Defizite und systembedingte Sicherheitslecks.

Der Zufall hilft manchmal der Wahrheit auf die Sprünge. Wenige Stunden vor der Vorlage der Bundestagstagesordnung, auf der das Gesetz zur Änderung des Bundeszentralregistergesetzes auftauchte, wurde eine Stellungnahme des Bundesrechnungshofs (BRH) bekannt, in der dieser mit deutlichen Worten bemängelte, dass es dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in mehr als zwei Jahren nicht gelungen sei, eine zertifizierte Software zur Nutzung der elektronischen Identität im neuen elektronischen Personalausweis zur Verfügung zu stellen.

Und wie hängt beides zusammen?

Das vorliegende Gesetz soll die – im Grunde ja wünschenswerte – Nutzung eines elektronischen Zugangs zu Führungszeugnissen und Auskünften aus dem Gewerbezentralregister eröffnen. Die bisher unbedingt vorgeschriebene persönliche Antragstellung wäre damit hinfällig.

Der Bundesrechnungshof schreibt dazu, dass zwar über 4 Mio. Euro ausgegeben worden sind, eine zertifizierte Software für den Identitätsnachweis der notwendigen Ausweis-App aber nicht vorliege.

Was ist die Folge?

Nach der Personalausweisverordnung sollen die Nutzer dieser Ausweis-App auf ihrem PC, Laptop oder anderem sicherstellen, dass sie nur eine vom BSI zertifizierte Software einsetzen, weil damit hinreichende Sicherheit gegeben sei. Tun sie das nicht – und das ist das Entscheidende – gehen sie

unkalkulierbare Haftungsrisiken ein. Sowohl was Datenverluste, als auch was kommerzielle Aktivitäten betrifft.

Laut BRH wurden die Nutzerinnen und Nutzer weder über die Nichtzertifizierung, noch über die damit verbundenen rechtlichen Probleme und Risiken, informiert. Die deutsche Rentenversicherung biete gar den elektronischen Zugang auf die Versichertendaten an und verweist – wahrheitswidrig – auf eine zertifizierte Ausweis-App des BSI.

In einer ersten Zusicherung hatte das BMI die Zertifizierung verbindlich zugesagt. Der BRH zitiert sie aber nun in dem Sinne, dass eine Zertifizierung in Ihren Augen nicht mehr nötig sei, da das BSI bei der Entwicklung der Software ja schon alles geprüft habe. Und „auftretende Schwachstellen (können) frühzeitig erkannt und zeitnah behoben werden“ (Saarbrücker Zeitung vom 22.04.2013).

Ich halte es ja tatsächlich für ein Problem, wenn die Software-entwickelnde Behörde, hier also das BSI, dieselbe ist, die das Produkt zertifizieren soll. So eine Interessenskollision haben wir im Gegensatz zu Ihnen immer kritisiert und vor den Folgen gewarnt.

Dass diese Konstruktion jetzt aber auch noch dafür erhalten muss, eine Zertifizierung ad acta zu legen, auf eine öffentlich nachvollziehbare Sicherheitsbewertung zu verzichten und die Nutzerinnen und Nutzer unwissend zu lassen, das ist schon ein ziemlicher Hammer.

Dieses Vorgehen entspricht aber – und damit zurück

zum vorliegenden Gesetz und dem nächsten Systemproblem – dem standardisierten fahrlässigen Umgang dieser Bundesregierung mit zum Teil hochsensiblen Daten der Bürgerinnen und Bürger:

Schon auf der ersten Seite der Gesetzesbegründung wird nämlich auf die neuen Regelungen des „Gesetzes zur Förderung der elektronischen Verwaltung ...“ (BT-Drs. 17/11473) verwiesen. Dieses erst vor wenigen Tagen verabschiedete sogenannte eGovernmentgesetz basiert auf dem De-Mailgesetz und der damit verbundenen unsicheren Technik. Ein hochgefährlicher Systemfehler der angestrebten elektronischen Verwaltung. Auf der Sachverständigenanhörung wurde das ausgesprochen anschaulich dargestellt. Die Bundesregierung wollte das nicht ändern und senkte stattdessen die Sicherheitsstandards in den Behörden zur Weitergabe von Daten ab.

Eine kleine Zwischenbilanz:

Das vorliegende Gesetz zwingt die Bürgerinnen und Bürger möglicherweise unsichere Technik einzusetzen und der Bundesregierung zu glauben, dass das schon in Ordnung gehe.

Dasselbe Gesetz fußt in einer Regelung – des Umgangs mit dem Geburtsnamen – auf dem gerade erst verabschiedeten Gesetz zur elektronischen Verwaltung, das wiederum auf der unsicheren De-Mail-Technik basiert.

Beide zusammen würden nicht funktionieren, hätte die Bundesregierung nicht das unsichere Projekt der

eID auf dem neuen Personalausweis gegen alle Kritik auf Biegen und Brechen ohne jede Notwendigkeit durchgesetzt.

Kaum eines der Versprechen nach optimaler Datensicherheit in den Großprojekten der Regierung konnte eingehalten werden. Alle - bis auf das in aller Schönheit gestorbene ELENA - wurden und werden jetzt im Endstadium der Legislaturperiode durchgedrückt. Um vollendete Tatsachen zu schaffen und im Dienste wirtschaftlicher Interessen.

Ich erinnere hier nur an den ePerso, eGovernment, ePass und elektronische Gesundheitskarte.

Dagegen steht die Vernunft der Bürgerinnen und Bürger:

17,5 Millionen Personalausweise mit eID-Funktion wurden bis Oktober 2012 ausgegeben.

Bei 70 Prozent davon haben klugerweise die AusweisinhaberInnen die eID-Funktion ausschalten lassen. Denn noch kann man das, obwohl immerhin 130 behördliche und kommerzielle Internetdienste damit anzupapfen wären.

Hier zeigt sich korrektes bürgerliches Misstrauen. Die Regierung scheint darauf zu setzen, durch vollendete Tatsachen und immer mehr per gesetzlichem Zwang eingeleitete Angebote dieses Misstrauen aus der Welt schaffen zu können.

Ich bin mir sicher, dass es sich dann eben anderswo wieder zeigen wird.

Vielen Dank.