Christoph Busch

Datensicherheit unerwünscht?

Wer würde es schon wagen, diese gerade für ein DuD-Heft provokante Frage zu stellen? Datenschützer, Juristen und Informatiker sind in der Regel bemüht, im konstruktiven Dialog gemeinsam Verfahren und Systeme zu entwerfen, zu entwickeln und zu installieren, die dem Datenschutz und der Datensicherheit Vorschub leisten. Dieses Anliegen sollte unabhängig davon verfolgt werden, ob der Betrieb des zu Grunde liegenden Basissystems die Zustimmung der beteiligten Parteien findet.

Nehmen wir eine in unserer Gesellschaft kontrovers diskutierte Fragestellung als Beispiel: Soll der Strombedarf unserer Bevölkerung und der in Deutschland ansässigen Industrie durch Kernkraftwerke oder durch alternative Stromquellen bedient werden? Darüber streiten sich die Geister und verschiedene Bundesregierungen der letzten Jahrzehnte kamen zu unterschiedlichen Entscheidungen. Es wurden Kernkraftwerke entwickelt und installiert. Es wurden deren Restlaufzeiten begrenzt und nun wieder verlängert.

Bei aller Unterschiedlichkeit der politischen Positionen sind sich jedoch alle Parteien darüber einig, dass die Datensicherheit der Steueranlagen der in Betrieb befindlichen Alt-Kraftwerke ein hohes Ziel ist, um das Risiko einer Umweltkatastrophe zu reduzieren. Der Angriff des Stuxnet-Wurms auf eine iranische Uran-Anreicherungsanlage im Sommer 2010 hat eindrucksvoll gezeigt, dass Steueranlagen mit einem hohen technischen Aufwand angegriffen werden können. Ein ähnlicher Angriff auf deutsche Atomkraftwerke kann nicht ausgeschlossen werden und so sind sich alle politisch und technisch Verantwortlichen im Anliegen einig, dass alle Maßnahmen ergriffen werden sollten, um dieses Risiko durch Datenschutztechniken zu reduzieren.

Dieser Konsens besteht unabhängig von der Frage, ob der Einzelne Kernkraftwerke grundsätzlich befürwortet oder nicht.

In diesem Heft werden aktuelle Anwendungsszenarien und Forschungsthemen zu biometrischen Verfahren vorgestellt und diskutiert. Auch über den Einsatz der Biometrie streiten sich die Geister quer durch die politischen Parteien. Während biometrische Verifikations-Systeme meist eine positive Bewertung finden, werden biometrische Identifikations-Systeme aus nachvollziehbaren Gründen von vielen Beteiligten abgelehnt. Als Argumente werden die hohen Risiken genannt, die sich aus den möglicherweise vorhandenen Zusatzinformationen in diesen persönlichen Daten oder aus unerwünschten Querbeziehungen ergeben. Aus diesen Überlegungen kam richtungsweisend Alexander Roßnagel in seiner Machbarkeitsstudie „Digitaler Personalausweis“ für die Bundesministerien für Wirtschaft und Technologie und des Inneren zu dem Ergebnis, dass zentrale Sammlungen biometrischer Daten in der Bundesrepublik Deutschland verfassungswidrig sind (s. Reichl/ Roßnagel/Müller (Hrsg.), Digitaler Personalausweis – Eine Machbarkeitsstudie, DuD-Fachbeiträge, 2005).

Bei aller Deutlichkeit, mit der seitdem zentrale Datensammlungen von Gesichtsbildern und Fingerbildern der Passantragsteller ausgeschlossen werden, gibt es de facto im Jahre 2011 in Deutschland zentrale Datensammlungen – und dies nicht nur für die forensische Arbeit des Bundeskriminalamtes. Zwei Beispiele seien hier genannt:

- Erstens wird im Juni 2011 die Europäische Union das Informationssystem über Visa-Antragsteller (Visa-Informationssystem VIS nach Verordnung EG Nr 767/2008) in Betrieb nehmen und dort Fingerbilder der betroffenen Personen zentral speichern. Dies beinhaltet auch diejenigen Personen, die einen Visa-Antrag in einer Auslandsvertretung der Bundesrepublik Deutschland gestellt haben.
- Zweitens werden vielerorts im privatwirtschaftlichen Umfeld zentrale Da-

tenbanken mit Fingerbildern von deutschen Bürgern aufgebaut, um im Einzelhandel ein bargeldloses Einkaufen zu ermöglichen. Eine große deutsche Einzelhandelskette verbreitet das System „Bezahlen mit dem Fingerabdruck“. Dieser Anwendung haben die betroffenen Personen freiwillig zugestimmt, um einen angenehmen Komfort nutzen zu können.

Unabhängig davon bestehen die Risiken, die Alexander Roßnagel für bundesdeutsche Sammlungen ausgemacht hat, gleichermaßen auch für EU-Sammlungen (wohlgemerkt unter deutscher Mitwirkung!) und für privatwirtschaftliche Sammlungen fort.

Wie beim eingangs genannten Kernkraftwerks-Beispiel sollte es doch auch hier politischer Konsens sein, dass die Erforschung und Entwicklung von Datensicherheit für zentrale biometrische Sammlungen ein gemeinsames Anliegen ist – unabhängig von der Frage, ob man diese zentralen Sammlungen befürwortet oder nicht. Dem Datenschutz und der Datensicherheit der betroffenen Personen würde mit einem Verzicht auf Forschung und Entwicklung ein Bärendienst erwiesen. Denn es gibt mit den Template-Protection-Verfahren, die in diesem Heft vorgestellt werden, hoffnungsvolle Perspektiven, auch für Identifikations-Systeme eine deutliche Verbesserung des Schutzniveaus zu erreichen.

Bleibt zu hoffen, dass die Bundesregierung die Entwicklung von Template-Protection-Verfahren angemessen fördert, selbst wenn biometrische Identifikations-Systeme politisch umstritten sind. Und weiterhin hoffen wir ebenso, dass kein Umweltminister die Datensicherheitsmaßnahmen für Kernkraftwerke aus Grundsatzfragen ablehnt. Datensicherheit ist und bleibt erwünscht – unabhängig davon, wie wir bereits existierende Basis-Systeme bewerten.