

1. Januar 2020:

- Pflicht für Bundesbehörden, ihre Akten elektronisch zu führen. Hinweis: Die die Behörden des Bundes betreffenden Regelungen zum sogenannten ersetzenden Scannen und zur Akteneinsicht treten am Tag nach der Verkündung in Kraft.

Neue Forschungsprojekte zu IT-Sicherheit in eingebetteten Systemen gestartet

„Internet der Dinge“ und „Industrie 4.0“ – diese zwei Begriffe stehen für die rasant fortschreitende Vernetzung unseres Lebens. Die Kommunikation zwischen Geräten und Maschinen – das „Internet der Dinge“ – entwickelt sich immer mehr zu einer Basis für das Funktionieren moderner Industriegesellschaften. Vor allem in der industriellen Produktion und der Telemedizin ermöglichen vernetzte intelligente Systeme, die in Maschinen und Geräte eingebettet sind, dass diese autonom miteinander kommunizieren. So werden völlig neue Funktionalitäten und Geschäftsmodelle möglich. Durch die zunehmende Vernetzung steigt aber auch das Risiko, dass diese Netzwerke Ziel von Cyberangriffen werden, die nicht nur erheblichen finanziellen Schaden verursachen, sondern auch die Funktionssicherheit technischer Anlagen bedrohen.

Im Kontext der 4. Ausschreibungsrunde des gemeinsam vom Bundesministerium für Bildung und Forschung und dem Bundesministerium des Innern initiierten Programms „IT-Sicherheitsforschung“ sind jetzt drei Forschungsprojekte an den Start gegangen, die neue Lösungen für eingebettete Systeme und eine hohe Sicherheit bei der Übertragung durch neue Verschlüsselungsmethoden zum Ziel haben. Beteiligt sind Hochschulen, Forschungseinrichtungen und Unternehmen.

Die drei geförderten Projekte in der 4. Ausschreibungsrunde:

- Um Angriffe auf industrielle Steuerungsrechner zu verhindern, wird im von der Wibu-Systems AG in Karlsruhe koordinierten Projekt Integritätsschutz eingebetteter Betriebssysteme (Projektvolumen: 2,21 Mio. Euro) eine neuartige Hardware-Architektur entwickelt, die einen vertraulichen und sicheren Betrieb von eingebetteten Betriebssystemen in einer offenen Internetumgebung sicherstellt.
- Ziel des Projekts Universell konfigurierbare Sicherheitslösung für Cyber-Physikalische Systeme (Projektvolumen: 1,56 Mio. Euro) ist eine universell konfigurierbare Sicherheitslösung für eingebettete Geräte und Systeme. Dabei geht es unter anderem um die Erkennung von Angriffen und Manipulationsversuchen. Koordinator ist die Hochschule Furtwangen.
- Das Projekt Effizientes Schlüsselmanagement für mehr Sicherheit im „Internet der Dinge“ (Projektvolumen: 3,37 Mio. Euro) widmet sich Sicherheitsfragen im „Internet der Dinge“. Um einen optimalen Schutz zu gewährleisten, werden neue Verfahren zur Verschlüsselung von Daten bei der Funkübertragung entwickelt. Das Projekt wird vom Fraunhofer Heinrich Hertz Institut in Berlin koordiniert.

Die Projekte laufen jeweils bis zum 31. August 2015.

Das Programm IT-Sicherheitsforschung ist im Jahr 2008 gestartet. Das Bundesministerium für Bildung und Forschung hat bisher insgesamt über 20 Forschungsvorhaben mit einem Gesamtvolumen von 30 Mio. bewilligt.

G&D: Elektronische Pässe mit neuem SAC-Zugriffsmechanismus

Die Republik Kosovo hat Giesecke & Devrient für die nächsten drei Jahre mit der Lieferung der neuesten Generation seiner elektronischen Reisepässe beauftragt. Zusätzlich zu den insgesamt 800.000 elektronischen Pässen liefert G&D eine moderne Systemlösung zur Pass-Personalisierung an das Innenministerium. Mit dieser Komplettlösung will die Republik Kosovo die Identität seiner Bürger durch den Einsatz modernster Sicherheitstechnologien künftig noch besser schützen. Mit der Entscheidung für die neuen Pässe setzt die Republik Kosovo europaweit einen Standard. Es sind die ersten Pässe mit dem neuen digitalen Zugriffsmechanismus SAC (Supplemental Access Control). Dieses Sicherheitsprotokoll ist in Europa ab Dezember 2014 bindend für alle neuen Passdokumente vorgeschrieben.

Die ersten Pässe sollen bereits vier Wochen nach Vertragsunterzeichnung an das Innenministerium geliefert werden. Jeder Pass enthält einen kontaktlosen Microprozessor, auf dem die persönlichen und biometrischen Daten der Inhaber gespeichert werden. Zudem werden die Fingerabdrücke der Bürger im Pass gespeichert. Das Extended Access Control-Verfahren (EAC) schützt die Daten vor unbefugtem Zugriff.

Die Lösung basiert auf G&Ds führendem, hoch performantem Betriebssystem für Reisepässe STARCOS 3.5, welches bisher als einziges weltweit für den gemeinsamen Einsatz von PACE und EAC sicherheitszertifiziert ist.

Die neue Generation von Passdokumenten für den Kosovo ist europaweit erstmalig mit dem neuen digitalen Zugriffsmechanismus SAC (Supplemental Access Control) ausgestattet. Dieser Mechanismus beruht auf dem kryptographischen PACE-Verfahren (Password Authenticated Connection Establishment) und zählt zu den sichersten verfügbaren Technologien. Dieser Zugriffsmechanismus ist in Europa erst ab Dezember 2014 bindend für alle EU-Mitgliedsstaaten vorgeschrieben.

Als weitere Neuerung wird weltweit erstmals auf einem Reisepass auch eine sogenannte CAN (Card Access Number) aufgedruckt sein. Diese erlaubt den abhörsicheren PACE-Zugriff auf die Passdaten durch manuelle Eingabe oder Scannen der CAN. Dieses Verfahren vereinfacht mobiles und gleichzeitig sicheres Auslesen der biometrischen Daten, zum Beispiel mit tragbaren Lesegeräten zur Identitätsprüfung. Zukünftig kann mit Hilfe der CAN und einem NFC-fähigen Smartphone mit entsprechender ID-App auch der Bürger die Daten auf seinem Reisepass selbst überprüfen.

Wie steht es um die elektronische Signatur in Deutschland?

Informationstag von TeleTrusT – Bundesverband IT-Sicherheit e.V. und VOI - Verband Organisations- und Informationssysteme e.V. am 19.09.2013 in Berlin.

Die Auswahl an Anwendungen für das elektronische Signieren ist breiter denn je und reicht von Verfahren mit Signaturkarten bis hin zu Angeboten für das Unterschreiben auf Tablets und Smartphones. Der Signaturtag 2013 bietet einen kompakten Überblick über Einsatzmöglichkeiten und die derzeitige rechtliche Situation.

Im Mittelpunkt der Vorträge stehen Erfahrungsberichte und Praxisbeispiele des Signatureinsatzes aus verschiedenen Branchen.