Strategische Offenheit

Dass die Unabhängigkeit von bestimmten Technologien, Plattformen und Herstellern oft nicht nur strategische, sondern auch sicherheitstechnische Vorteile verspricht, ist spätestens seit dem „I-love-you-Virus" bekannt. Auch die Bedeutung offener Standards und Schnittstellen für die Interoperabilität in komplexen technischen Systemen ist seit vielen Jahren klar. Vor diesem Hintergrund erfreuen sich offene, transparente und kooperative Ansätze zunehmender Beliebtheit und in der Software-Industrie hat sich „Open Source" als Entwicklungs-, Lizenz- und Geschäftsmodell in vielen Fällen als Standard etabliert.

Darüber hinaus werden vor dem Hintergrund aktueller Entwicklungen verschiedene Fragen aufgeworfen:

- Wie robust können Sicherheitssysteme überhaupt sein, bei denen neben wohldefinierten Schlüsselaspekten noch viele weitere technische und organisatorische Details geheim gehalten werden?
- Kann quelloffene Software gemäß anerkannter Sicherheitskriterien, wie z.B. Common Criteria, evaluiert und erfolgreich zertifiziert werden?
- Wäre die konsequente Veröffentlichung der Quellen darüber hinaus nicht sogar die Voraussetzung für buchstäblich vertrauenswürdige Plattformen und Systeme?

Das vorliegende Heft adressiert diese und verwandte Fragen im Umfeld der „Open Source Sicherheit" und beleuchtet einige aktuelle Entwicklungen in diesem Bereich. Dies umfasst neben der von Wilhelm Merx beleuchteten Nutzung von Open Source Technologien zur effizienten Entdeckung und Verwaltung von Schwachstellen und dem Einsatz von Open Source für das Cloud Computing in der „Deutschen Wolke" beispielsweise auch den Einsatz von quelloffener Software für elektronische Ausweise und Signaturen.

Der Beitrag von Tomas Gustavsson beantwortet die oben aufgeworfene Frage zur möglichen Common Criteria Zertifizierung von Open Source positiv und schildert die Erfahrungen bei der Evaluierung der quelloffenen EJBCA. Der Beitrag von Horsch & al. stellt die derzeit im Rahmen des von der Europäischen Kommission unterstützten FutureID-Projektes stattfindende Entwicklung eines quelloffenen eID- und Signatur-Clients auf Basis der Open eCard App und der an der TU Graz entwickelten Signaturbibliotheken vor. Mit der im PersoSim-Projekt entwickelten Software kann ein Personalausweis oder eine ähnliche Ausweiskarte simuliert werden, was zukünftig die Entwicklung und Qualitätssicherung von eID-Clients deutlich erleichtern dürfte. In eine ähnliche Richtung, nämlich auf die Steigerung der Transparenz und Interoperabilität im Bereich elektronischer Ausweise und Signaturen, zielen schließlich das „Common eID" Projekt und die von namhaften Europäischen Institutionen, Verbänden, Projekten und Unternehmen unterstützte „Open Signature Initiative".

Die verschiedenen Projekte belegen nicht nur den strategischen Vorteil der „Open Source Sicherheit", sondern liefern darüber hinaus in den verschiedenen Bereichen auch handfeste praktische Verbesserungen.

Nutzen Sie die vorgestellten Entwicklungen und die Freiheit sich an diesen offenen und gemeinnützigen Initiativen beteiligen zu können!

Detlef Hühnlein