



Forschung insight

Informatik . Forschung . Paderborn

Kein Weg führt zum Profil Datenschutz im digitalen Rechtemanagement

Nutzerprofile – sie entstehen durch Transaktionen im Internet und werden für Marketing und Vertrieb generiert. Was für die einen hochinteressant, ist bei vielen Nutzern unerwünscht. Auch Software-Lizenzen – installiert auf dem privaten Rechner – bieten eine breite Informationsfläche: Lizenzgeber können die Software-Nutzung beobachten und Informationen zusammenstellen. Bei der Variante des Cloud Computing wird die Software in einem Rechenzentrum innerhalb der Cloud installiert. Hier können Nutzerprofile sogar noch detaillierter erstellt werden. Das geht vielen Nutzern zu weit – und widerspricht dem Datenschutz.

Die Fachgruppe „Sicherheit in Netzwerken“ um Jun.-Prof. Christoph Sorge und sein Mitarbeiter Ronald Petrlic verfolgen einen neuen Ansatz – mittels On-the-Fly Computing, die Zukunftsversion des Cloud-Computing. Ihre Idee ist die Trennung zwischen Software-Anbieter, dem ausführenden Rechenzentrum und der Bezahlung. Obwohl sich Lizenzgeber wie auch das Rechenzentrum wie gehabt in der Cloud befinden, gibt es zwischen den Beteiligten keine gemeinsamen Informationskanäle: Die Anbieter arbeiten mit einem digitalen Rechtemanagement, die Nutzer sind datenschutzrechtlich vollständig abgesichert. Es wird nicht mehr möglich sein, direkt oder über den Dritten Informationen über die Software-Nutzung zu sammeln – ein Nutzerprofil kann somit nicht mehr erstellt werden.

Dass weder Anbieter noch Rechenzentrum Informationen über die Nutzung erhalten, der Lizenzgeber gleichzeitig

jedoch Sicherheit über die erlaubte Dauer und Art und Weise der Nutzung seiner Software erhält, klingt wie ein Widerspruch. Aber genau diesen wollen Sorge und Petrlic auflösen und beide Aspekte miteinander vereinbaren.

Um das digitale Rechtemanagement umzusetzen, integriert die Fachgruppe

die sie für ihre eingeschränkte Aktion benötigen – ein Datenaustausch darüber hinaus ist technisch unmöglich.

Für das Lizenzmanagement hat die Fachgruppe eine eigene Smart Card implementiert. Sie dient zum Kauf der Software-Lizenz und ist als sichere Hardware ein „Vertrauensanker“: Nur Berechtigte können, im Rahmen ihres begrenzten Zugriffs, die Daten auslösen.

Das Konzept und die Programmierung der einzelnen Bausteine sind abgeschlossen. Gegenwärtig folgt die Implementierung einzelner kryptografischer Verfahren zu einem größeren Gesamtsystem. Die entsprechenden Verschlüsselungsverfahren liefert die Fachgruppe „Codes und Kryptografie“ um Prof. Johannes Blömer. In Zukunft werden dann auch spezielle rechtliche Aspekte von Bezahlverfahren berücksichtigt.

Die Entwicklungen sind Bestandteil des Sonderforschungsbereiches (SFB) 901 „On-The-Fly Computing“.



Digitales Rechtemanagement bei Software-Lizenzen: Ronald Petrlic versperrt Nutzerprofilen den Weg

ein anonymes Bezahlverfahren, für das die Nutzer keine Kreditkarte mehr benötigen: Sie registrieren sich an einer virtuellen Bank in der Cloud und erhalten daraufhin „digitale Münzen“ – Zeichenketten, die bestimmte Daten über Geldbeträge enthalten. Mit diesen Münzen kauft der Nutzer die Software beim Lizenzgeber. Er bezahlt jedoch nicht dort, sondern löst sie bei der Bank ein. Diese kann den ursprünglichen Nutzer durch Verschlüsselungsverfahren nicht mehr identifizieren. Anschließend übergibt der Nutzer die Software dem Rechenzentrum zur Installation. Anbieter, Rechenzentrum und Bank verfügen jeweils ausschließlich über exakt die Informationen,

Kontakt:
Ronald Petrlic, M.Sc.
Sicherheit in Netzwerken
05251 60-1764
ronald.petrlic@uni-paderborn.de