Abstract anhand eines Beispielthemas

Neue Herausforderungen für die IT Sicherheit in Big Data Systemen

Die Auswertung von großen, unstrukturierten Datenmengen in Echtzeit ist zu einer der zentralen Aufgaben der Informationstechnologie geworden. Software wird zunehmend nicht mehr auf dem klassischen Wege vermarktet, sondern kostenlos angeboten. Das Geschäftsmodell hinter solchen Angeboten ist die Sammlung von Nutzerdaten und das generieren von neuen Erkenntnissen zu Verhalten und Vorlieben der Nutzer. Die Anbieter kostenloser Software erhoffen sich, mit diesen Erkenntnissen Gewinne zu generieren. Die persönlichen Daten der Nutzer und daraus abgeleitete Informationen lösen Geld als klassisches Zahlungsmittel ab und werden verstärkt als Ware gehandelt.

Die Nutzer sind dabei häufig nicht darüber informiert, wie ihre Daten gesammelt, verarbeitet und weiter gegeben werden. Zwar schreibt der Gesetzgeber vor, die Nutzer über den Datenhunger von Anwendungen aufzuklären, doch werden diese Hinweise bei der Installation von Anwendungen allzu oft ungelesen akzeptiert.

Auch an die Absicherung von IT Systemen stellt Big Data neue Anforderungen. Es ist nicht mehr länger möglich, eigene Systeme durch Absicherung der Perimeter vor Angriffen von außen zu schützen, da Daten von Endgeräten gesammelt werden, über die der Hersteller keine direkte Kontrolle hat. Um eine so große Datenmenge effizient und in Echtzeit bearbeiten zu können, sind außerdem verteile Systeme notwendig, die sich nicht physikalisch an einem bestimmten Ort befinden.

Wir gehen zunächst auf die speziellen Anforderungen von Big Data Systemen ein und zeigen, inwiefern sich diese Anforderungen von denen herkömmlicher zentral verwalteter Systeme unterscheiden. Nachdem anschließend die zentralen Aspekte von Privacy nach der EU Direktive von 2015 eingeführt wurden, beschreiben wir den aktuellen Stand der Forschung bezüglich technischer Maßnahmen zum Schutz der Privatsphäre der Nutzer. Wir zeigen die Diskrepanz zwischen den Anforderungen und dem Stand der Technik am Beispiel von Spaß und leiten anschließend neue technische Maßnahmen zum Schutz der Privatsphäre von Nutzern her.

In der Evaluierung zeigt sich, dass die verschlagenen Maßnahmen effektiv sind, und sowohl die Transparent für die Nutzer sind als auch das Risiko eines Datenlecks reduzieren. In der Simulation von verschiedenen Angriffen konnte gezeigt werden, dass die erweiterten Sicherungsmechanismen zur datenzentrierten Sicherheit (Data Centric Security) zwar keine Angriffe verhindern könne, jedoch dafür sorgen, dass ein Angreifer aus den gestohlenen Daten keine Informationen mehr erhält. Der kombinierte Einsatz verschiedener Sicherungsmechanismen steigerte in unseren Tests zusätzlich die Datensicherheit, womit gezeigt werden konnte, dass ein einzelnes Konzept zur Schutz der Privatspäher nicht ausreichend ist.