Rezension

M.F. Dennedy, J. Fox, T.R. Finneran:
The Privacy Engineer's Manifesto
Apress, 2014

„The Privacy Engineer's Manifesto" ist ein Buch darüber, wie man gängige Requirements Engineering-Techniken für die Ermittlung und Spezifikation von Datenschutz-Anforderungen einsetzen kann. Aus den Unternehmens- und Benutzerzielen werden Privacy Policies hergeleitet und daraus die Anforderungen an das IT-System. Daraus leiten sich ein Datenmodell, Arbeitsprozesse, (technische) Privacy-Mechanismen und System-Architektur her. Schulungen und Qualitätsmanagement gehören ebenfalls zum „Privacy Engineering Development Process", der durch Rückmeldungen und Nachbesserungen aus der Qualitätssicherung zum Kreislauf wird. Textuelle Use Cases dienen dabei als Gedankenexperiment für alternative Szenarien, deren Nutzen und Risiken. Aus Datenschutzgesetzen folgen konkrete, wiederverwendbare Anforderungen wie z. B. dass personenbezogene Daten eine Verknüpfung zu einem Zweck haben müssen und dass Benutzer über die Verarbeitung ihrer Daten informiert werden und dieser ausdrücklich zustimmen.

Das empfohlene Vorgehen wird schrittweise anhand eines konkreten Beispiels dargestellt. Dadurch wird es leicht nachvollziehbar und umsetzbar. Das Ziel der Autoren besteht darin, wiederholbare Ingenieurprinzipien zu definieren, um zu vermeiden, dass Datenschutz eine händisch definierte einmalige Sache bleibt.

Als Grundprinzipien des Privacy by Design definieren die Autoren:

1. Proactive, not reactive: preventative, not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

Das Buch enthält außerdem – daher der Titel – ein Manifest des „Privacy Engineers" mit zehn Prinzipien über die Bedeutung personenbezogener Daten. Laut dem Manifest ist jeder ein Privacy Engineer (Datenschutz-Ingenieur). Es definiert Grundeinstellungen, Fähigkeiten und Arbeitsweisen für diese Tätigkeit: Kreativität und Kommunikationsfähigkeit, technische und Soft Skills, Lernen aus der Vergangenheit, Vermeiden von Schaden, Verstehen, Verringern und Akzeptieren von Risiken. Innovation und Komplexität sind keine Probleme für den Privacy Engineer, aber eine unzureichende Vorstellungskraft schon.

Ein Problem des Datenschutzes besteht darin, dass Daten erhoben werden müssen, um Daten zu schützen ("It takes data to protect data." S. 21). Um zu ermitteln, ob bzw. welche Datenschutzregeln gelten, müssen Daten über Kunden und deren Kommunikationspartner gesammelt werden. Auch der Prozess der Qualitätssicherung muss auf die Einhaltung von Datenschutzregeln geprüft werden.

Daten, die früher als unpersönliche Maschinendaten galten, werden neuerdings personenbeziehbar, beispielsweise durch IoT (Internet of Things). Das Buch definiert als „IoT Privacy Maxim" (S. 18f), dass Informationen dann personenbeziehbar sind, wenn einer gemessenen Aktivität die Identität einer Person zugeordnet werden kann oder wenn Identitäts- und Aktivitätsinformationen in derselben Datenbank vorliegen.

Dieses Buch ist interessanter und nützlicher Lesestoff für diejenigen, die datenschutzkonforme IT-Systeme entwickeln oder sich allgemein für das Thema interessieren. Die Autoren haben ein systematisches, allgemeingültiges Vorgehen entwickelt und zahlreiche gute Gedanken im Sinne der Softwaretechnik gesammelt.

rezensiert durch Andrea Herrmann