erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Werner Hülsmann

Datenschutz – Ein Qualitätsmerkmal bei der Softwareentwicklung?

Erwartung der Kunden versus Wirklichkeit der Hersteller

Wenn betriebliche Datenschutzbeauftragte nach der Berücksichtigung des Datenschutzes bei der Auswahl der Software fragen, bekommen sie oft zu hören: „Das Produkt wird doch in Deutschland verkauft, da wird es schon deutschen Datenschutzanforderungen genügen", oder „Das Produkt wird auch von der Firma (beliebiger größerer Konzern) eingesetzt und wenn die das einsetzen wird das schon in Ordnung sein."

Kaum eine Software, kaum ein EDV-System, kommt heute ohne die Speicherung personenbezogener Daten aus. Egal ob es sich um die Daten der Beschäftigten oder um die personenbezogenen Daten in den Bereichen Vertrieb und Marketing handelt: In den meisten Fällen kommt Standardsoftware zum Einsatz, die je nach Softwareprodukt und Unternehmen nur noch mehr oder weniger stark an die jeweilige Firma angepasst wird. Dabei sind große Änderungen in der Praxis kaum möglich, da diese zu einem unverhältnismäßig hohen Aufwand bei den regelmäßigen Updates führen würden.

Nicht nur in mittelständischen Unternehmen, sondern auch in mittleren und größeren Konzernen ist leider noch häufig die irrige Meinung vertreten, dass Softwareprodukte, die auf dem deutschen oder europäischen Markt angeboten werden, sich ohne weiteres datenschutzkonform einsetzen lassen. Die Erfahrung aus der Praxis zeigt allerdings, dass Standardkonfigurationen zu einem nicht datenschutzkonformen Einsatz führen, oder dass gar unabhängig von der Konfiguration ein datenschutzkonformer Einsatz nur mit einem unverhältnismäßig hohen Einsatz oder gar nicht möglich ist.

Warum ist Datenschutz nicht standardmäßig implementiert?

Diese Frage stellen sich Datenschützerinnen und Datenschützer schon seit Jahren oder sogar Jahrzehnten. Ein häufig – gerade von großen Softwareschmieden – angebrachtes Argument ist, dass es ja nicht möglich sei, für jedes Land eine eigenständige Version zu „stricken". Dieses Argument ist allerdings spätestens seit 1995, dem Jahr, in dem die EG-Datenschutzrichtlinie in Kraft trat, nicht mehr stichhaltig. Weitere Datenschutzrichtlinien sind hinzugekommen. Die EG-Datenschutzrichtlinien dienen ja ausdrücklich dazu, um den Austausch von Waren und Dienstleistungen innerhalb der inzwischen 25 Staaten der EU und dem Europäischen Wirtschaftsraum (dem zusätzlich Island, Liechtenstein und Norwegen angehören) zu erleichtern. Dieser „Europäische Datenschutzraum" aus 28 Staaten stellt einen beachtlichen Markt auch für Software dar. In all diesen Staaten muss sich der Datenschutz an den EG-Richtlinien zum Datenschutz orientieren. Sicher gibt es gewisse Unterschiede in der Umsetzung. In Spanien gilt beispielsweise für die werbliche Nutzung ein generelles Opt-Out-Prinzip, in Deutschland gilt dagegen in vielen Bereichen ein Opt-In-Prinzip. Allerdings lassen sich diese Unterschiede nun wirklich durch entsprechende Konfigurationsmöglichkeiten realisieren und sind kein Argument dafür, die Kennzeichnung von Werbeeinwilligungen oder Werbewidersprüchen auf ein Freitextfeld zu verbannen.

Ein anderes oft gehörtes Argument der Softwarehersteller ist: „Die Kunden sind nicht bereit, für den Datenschutz zu bezahlen". Dies mag dann gelten, wenn die Entwicklungskosten für etwaige Datenschutzergänzungen dem einzelnen Kunden für seine Version vorgehalten werden und bei der Preisgestaltung nicht berücksichtigt wird, dass diese Datenschutzergänzungen bei allen künftigen Verkäufen in der EU und dem Europäischen Wirtschaftsraum zur Geltung kommen. Dem auch oft genannten Argument: „Die Kunden fragen nicht nach Datenschutz",

kann nur entgegengehalten werden, dass – wie eingangs dargestellt – viele Firmen davon ausgehen, dass eine Software, die sie in Europa einkaufen, auch den europäischen Datenschutzstandards entspricht. In vielen anderen Bereichen ist es ja auch so. So darf in Deutschland ein KFZ nur dann verkauft werden, wenn es der deutschen Straßenverkehrszulassungsverordnung entspricht oder deutlich als nur für den Export gedacht angeboten wird. Auch Elektrogeräte dürfen nur in den Handel gebracht werden, wenn sie bestimmten Sicherheitsanforderungen genügen. Software hingegen darf in den Handel gebracht werden, auch wenn sie den einfachsten Datenschutzanforderungen nicht genügt.

Was sind die Datenschutzanforderungen an die Software?

Um als Softwareentwicklungsfirma zu wissen, welche Anforderungen eine Software aus Sicht des Datenschutzes erfüllen muss, genügt eigentlich ein Blick in das Gesetz, insbesondere in die Anlage zu § 9 des Bundesdatenschutzgesetzes (BDSG). Dort werden so genannte technische und organisatorische Maßnahmen (TOM) gefordert, um acht Schutzziele zu erreichen. Manchmal genügt auch die Lektüre der Tagespresse. So ist eine ganz wesentliche Grundanforderung: Die Software muss so geschrieben sein, dass das Administrationspasswort nach der Installation vom Administrator zwingend geändert werden muss. Wäre dies berücksichtigt worden, wäre unter anderem das Datenleck bei vielen Einwohnermeldeämtern vermieden worden.

Wenn eine Quasi-Standardsoftware für Hotels nicht über eine ausreichende Zugriffsrechteverwaltung verfügt, ist das aus datenschutzrechtlicher Sicht bedenklich. Wenn allerdings weit verbreitete Software für Arztpraxen Patientendaten unverschlüsselt auf den Festplatten speichert und dem – meist externen – Administrator volle Einsicht in die Patientendaten gewährt, dann ist dies schon kriminell!

Hier seien nur einige Anforderungen stichwortartig aufgeführt (die Aufzählung kann an dieser Stelle nicht vollständig sein):

- Passwörter müssen so eingerichtet werden können, dass
  - sie nach der ersten Anmeldung verpflichtend geändert werden müssen,
  - sie eine Mindestlänge von acht bis 12 Zeichen haben müssen,
  - sie aus eine Kombination von Buchstaben sowie Ziffern und/oder Sonderzeichen bestehen,
  - sie eine maximale Gültigkeitsdauer zwischen 30 und 90 Tagen haben können, und
  - bei Änderung die letzten drei bis 12 Passwörter nicht wiederverwendet werden können.
- Zugriffsberechtigungen müssen so eingerichtet werden können, dass
  - das Vier-Augen-Prinzip zumindest für wesentliche administrative Aufgaben realisiert werden kann,
  - die Aufgabenverteilung innerhalb der verantwortlichen Stelle durch das Berechtigungskonzept nachgebildet werden kann, und
  - Berechtigungen zeitlich beschränkt werden können,
  - Speicherung der Daten sowie die Datensicherung in verschlüsselter Form möglich sind.
- Die Änderung von Daten sollte mitprotokolliert werden können. Dabei
  - müssen die Zugriffsrechte auf das Protokoll so eingestellt werden können, dass auch hier ein Vieraugenprinzip umgesetzt werden kann,
  - muss das Protokoll revisionssicher sein, und
  - muss das Protokoll so eingerichtet werden können, dass nur Änderungen an wesentlichen Daten protokolliert werden.
- Die Software muss die Löschung personenbezogener Daten rückstandsfrei ermöglichen.
- Bei Kundendaten müssen Werbesperrvermerke eingetragen werden können.
- EDV-Systeme sollten den Einsatz einer chipkarten- oder noch besser einer zertifikatsbasierten Zugriffskontrolle unterstützen.
- Bei Programmen, bei denen Datenübermittlungen vorgesehen sind, ist sicherzustellen, dass die Datenübermittlungen
  - verschlüsselt erfolgen und
  - protokolliert werden können.

Werner Hülsmann

Werner Hülsmann, Diplom-Informatiker mit Schwerpunkt Datenschutzrecht, Jahrgang 1961, Inhaber von Datenschutzwissen.de und selbstständiger Datenschutzberater, ist seit 2004 beim unabhängigen Datenschutzzentrum anerkannter Sachverständiger für IT-Produkte (rechtlich, technisch) und Kooperationspartner des virtuellen Datenschutzbüros. Er ist Vorstandsmitglied der Deutschen Vereinigung für Datenschutz (DVD) e.V., Bonn und des FIfF e.V., Bremen.

- In Datenbanksystemen muss der Zweck der erstmaligen Speicherung und die Herkunft der Daten hinterlegt werden können.

- Bei Kundendaten müssen Werbewidersprüche oder noch besser Werbeeinwilligungen für unterschiedliche Kanäle (Post, Telefon, FAX, E-Mail, SMS) hinterlegt werden können.

- Bei Personaldatenbanken müssen für unterschiedliche Felder unterschiedliche Berechtigungen vergeben werden können. Die Reisekostenstelle muss keinen Zugriff auf Gehaltsdaten oder gar Lohnpfändungen oder Gesundheitsdaten haben.

- Die Auskunft über alle zu einer Person gespeicherten Daten muss einfach und rasch umsetzbar sein.

Diese Liste muss für die konkrete Anwendung unbedingt ergänzt werden. Hier sind die betrieblichen und behördlichen Datenschutzbeauftragten gefordert. Ihre Aufgabe ist es, dafür zu sorgen (oder darauf „hinzuwirken", wie es der Gesetzgeber nennt), dass bereits in das Pflichtenheft die Anforderungen zur Umsetzung des Datenschutzes aufgenommen werden und nicht darauf vertraut wird, dass nur datenschutzkonforme Software angeboten würde.

Nur wenn die Softwarehersteller und -anbieter regelmäßig mit den datenschutzrechtlichen Anforderungen konfrontiert werden, werden sie erkennen, dass die die Einhaltung und Umsetzung des Datenschutzes nicht nur von den Kunden – zu Recht – erwartet wird, sondern auch ein wesentliches Qualitätsmerkmal darstellt.

Fazit

Zurzeit können sich Kunden nicht darauf verlassen, dass selbst Software von großen renommierten Anbietern den datenschutzrechtlichen Anforderungen genügt. Vielmehr müssen Firmen, Behörden und Institutionen, die Software einkaufen wollen, bereits bei der Ausschreibung oder der Angebotseinholung die Umsetzung des Datenschutzes in das Pflichtenheft aufnehmen. Wünschenswert wäre es allerdings, dass Software, die für den nicht unbeachtlichen europäischen Markt entwickelt wird, bereits in der Grundkonfiguration so eingerichtet ist, dass sie den wesentlichen datenschutzrechtlichen Anforderungen genügt.