Produktdokumentation

Version	Final 02
Datum	22.01.2003
Autoren	LD 6.1 Dr. Sharam Gharaei LD 6.2 Irina Bruns LD 9 Dr. Anja Diek LD 9.1 Peer Reymann
Kontakt:	mail@datenschutzzentrum.de

Produktdokumentation

Das wichtigste Hilfsmittel in der Vorbereitungsphase ist die Überprüfung der Produktdokumentation.

Eine Dokumentation ist nur dann brauchbar, wenn sie **aktuell**, vom **Umfang** her ausreichend, von der **Abdeckung** her vollständig und von der **Darstellung** her aufschlussreich ist. Dabei ist jedoch zu bemerken, dass eine sinnvolle Produktdokumentation in Abhängigkeit des Produktes einen sehr unterschiedlichen Umfang haben kann. Unter Berücksichtigung der notwendigen Qualität des zu erstellenden Gutachtens und der für den praktischen Einsatz des Produkts im täglichen Betrieb notwendigen Handbücher, sind hier Augenmaß und eine pragmatische Herangehensweise gefordert.

Beispielsweise wird die Produktdokumentation bei einer Netzwerkkomponente, wie einem Router, der mit umfangreichen Sicherheits-Komponenten ausgestattet sein kann, sicherlich dennoch einen geringeren Umfang und einen anderen Fokus haben, als dies bei einem Arztpraxissystem zur Verwaltung der Patientendaten und zur Erstellung von Abrechnungen der Fall sein dürfte.

Generell sollte die mitgelieferte Dokumentation ausreichend präzise und umfangreich sein, um einem Verfahrensbetreuer bzw. Administrator eine nach wertender Gesamtbetrachtung datenschutzgerechte Konfiguration des Produktes zu ermöglichen. Auf die Veröffentlichung „Das schleswig-holsteinische Datenschutzgütesiegel“, Stand: 2002-02-01, V 1.0, Seite 15 ff. des ULD wird verwiesen.

Klassifizierung von Bestandteilen der Produktdokumentation

Anhand der Dokumentation können essentielle Informationen für den Begutachtungsprozess bereits vorbereitend ausfindig gemacht werden. Dazu gehören:

- Feststellung der Datenarten
- Funktionalität
- Architektur des Produktes
- der vorgesehene Kontext bzw. das Einsatzgebiet

Da Produktdokumentationen aus höchst unterschiedlich gegliederten und auch inhaltlich sehr unterschiedlichen Dokumenten bestehen können, haben wir die folgenden Kategorien von Dokumentationsbestandteilen definiert:

Typ	Beschreibung
T1	in Lieferumfang enthalten und Gegenstand der Begutachtung[i]
T2	Pflicht-Dokumente, die nicht zum Lieferumfang gehören, aber auf Anforderung des Sachverständigen vom Hersteller zur Verfügung gestellt werden müssen

T3	Pflicht-Dokumente, die nicht zum Lieferumfang gehören, aber u.U. zur Verfügung gestellt werden müssen (in Abhängigkeit vom Produkt)
T4	Optionale Dokumente, die der Hersteller freiwillig bereitstellen kann

Die Dokumente der Kategorie T1 sind sogenannte „Muss-Bestandteile“ einer Produktdokumentation. Anhaltspunkt für den Umfang der in jedem Fall bereitzustellenden Dokumentation der Kategorie T1 ist aus unserer Sicht die Menge an Informationen, die in einer einsetzenden Stelle auf jeden Fall benötigt wird, um das Produkt von einem Administrator ordnungsgemäß zu installieren, zu testen, in ein Verfahrensverzeichnis einzuführen und in den Echtbetrieb nehmen zu lassen. Hierbei kommen auch die Vorschriften der DSVO zum Tragen, denn auch dort wird ein Mindestmaß an Dokumentation beim Einsatz in Behörden definiert. Des weiteren von Bedeutung für den datenschutzgerechten Einsatz ist das technisch-organisatorische Einsatzmodell, das konkrete Anhaltspunkte für die Praxis geben soll und in dem ggfs. leichte technische Schwächen des Produktes durch organisatorische Maßnahmen ausgeglichen werden können.[1]

Die Dokumente der Kategorie T1 müssen auf jeden Fall vom Lieferumfang her dem Anwender die Möglichkeit zum datenschutzgerechten Einsatz des Produktes geben. Dafür kann es im Einzelfall erforderlich sein, dass der Hersteller die Dokumentation vom Typ T1 auf Verlangen des Sachverständigen um weitere Dokumentationsteile ergänzt. Trotzdem dürfen die Dokumente vom Typ T1 nicht von dem Sachverständigen erstellt werden, um die gutachterliche Unabhängigkeit zu wahren.

Minimalanforderung im Bereich Risikoaufklärung ist die Dokumentation von (auch möglicherweise einsatzabhängigen) Schwachstellen und Folgen der Parametrisierung des Produktes im Hinblick auf die Anforderungen des Datenschutzes (Anlage zu §9 BDSG, Datenvermeidung, Datensparsamkeit etc.).

Als „vorbildlich“ wird angesehen, wenn Dokumente der Gruppe T1 mindestens eine kurze Risikoanalyse enthalten. Hierunter verstehen wir die Zusammenstellung aller inherenten Schwachstellen des Produktes und aller Angriffspotentiale, die sich aus der typischen Einsatzumgebung ableiten, deren Bewertung und Hinweise für deren Vermeidung. Darüber hinaus sind die anzuwendenden Verfahren zur Wahrung der Rechte des/der Betroffenen – wie erhält diese/r Auskunft über die gespeicherten Daten? / wie erfolgt ggfs. die Auswertung einer Weitergabekontrolle? – ausführlich darzustellen.

[1] Aus den bisherigen Erfahrungen lässt sich ableiten, dass offene Schnittstellen zum Datenim- und Export regelmäßig aus datenschutzrechtlicher Sicht eine Schwachstelle eines Programms darstellen, da auch anonymisierte oder pseudonymisierte (Teil-)datensätze mithilfe externer Anwendungen (auch sog. Office-Produkte) in unzulässiger Weise automatisiert so zusammengesetzt werden können, dass ein Rückschluß auf die gespeicherten Daten (=Personenzuordnung) möglich wird.

Wenn im Gutachten zur Zertifizierung des Produktes eine Beschränkung der Untersuchung auf eine festgelegte Konfiguration erfolgt, so ist diese in der T1-Dokumentation umfassend und nachvollziehbar zu beschreiben.[1]

Während die Gruppen T1, T2 und T3 eine konkrete Eingrenzung bilden, ist der Dokumenttyp T4 weit gefasst. Der Grund dafür ist, dass die vorgenommene Kategorisierung der Produktdokumentation für verschiedene Produktarten verwendbar sein soll und Offenheit für unterschiedliche Formen von Produktdokumentation bewahrt werden soll. Je nach Produktart könnte eine bestimmte Dokumentation als obligatorisch oder optional betrachtet werden[ii]. Das könnte auch für Produkte der gleichen Art gelten.[iii]

Hinweise für die notwendige Dokumentations- und Prüftiefe ergeben sich konkret aus den vom Produkt tangierten Rechtsgebieten: im Bereich der Bearbeitung von Sozialdaten mit abschließend geregelten Datenprofilen ist beispielsweise die Vorhaltung von anderen als den gesetzlich vorgesehenen Datenfeldern, insbesondere Freitextfeldern, unzulässig und muß ggfs. auf Niveau der Datenbankdefinition nachgewiesen werden. Geht die Datenbank über das gesetzliche Profil hinaus, so sind die notwendigen Sicherungs- und Konfigurationsmaßnahmen detailliert zu beschreiben. Die Anwendung von Prüf- und Dokumentationspflichten in Anlehnung an das Normenwerk „Common Criteria“ (CC) wird durch das ULD angestrebt.

Es soll auch beachtet werden, dass die Dokumente vom Typ T2, T3 und T4 i.d.R. nur direkt vom Hersteller zu beziehen sind und nicht als Begleithandbuch mit dem Produkt geliefert werden.

Anhand der obigen Differenzierung werden folgende Produktdokumentationen empfohlen:

T1: Dokumente, die in Lieferumfang enthalten sein müssen:

- Administrationshandbuch
- Benutzerhandbuch
- Aktuelle Informationen über Schwachstellen, besser: Risikoanalyse
- Installation, Erzeugen, Initiierung und Revision/Prüfung der Sicherheits-prozeduren
- High-level-Entwurf (Architektur und Module)
- Technisch-organisatorisches Einsatzmodell einschließlich Hinweisen für Verfahrensbetreuer

Die aufgeführten Dokumente müssen im Einzelfall nicht vollzählig mit den oben genannten Titeln vorhanden sein. Hier ist wiederum Augenmaß gefordert, denn wichtig ist vor allem, ob die Funktionalität, die ein Dokument im Einzelnen haben soll, insgesamt erfüllt ist. Beispielsweise könnte produktspezifisch

[1] Die zum Teil erhebliche Vielzahl von Konfigurations- und Parametrisierungsmöglichkeiten gerade auch der zugrunde liegenden Basissysteme (Betriebssystem, Netzwerk, Datenbank etc.) führt erfahrungsgemäß dazu, dass mit Rücksicht auf den Umfang der Untersuchungen nur eine begrenzte Anzahl von Musterkonfigurationen prüfbar ist.

Administrations- und Anwenderhandbuch zu einem Handbuch zusammenfallen, wenn alle Informationen, die man in den Handbüchern üblicherweise erwartet, vorhanden sind.

T2: Pflicht-Dokumente, die nicht zum Lieferumfang gehören, aber auf Anforderung des Sachverständigen vom Hersteller zur Verfügung gestellt werden müssen:

- Konfigurationsmanagement
- aktuelle funktionale Spezifikation einschließlich der verwendeten Datenmodelle
- Aufbau und Bestandteile des Produktes

T3: Pflicht-Dokumente, die nicht zum Lieferumfang gehören, aber u.U. zur Verfügung gestellt werden müssen (in Abhängigkeit vom Produkt)

- Schwachstellenanalyse (*Vulnerability Assessment*) (im Falle leichter Angriffe).
- Vollständige Darstellung der Implementation
- Analyse der Übereinstimmung zwischen der funktionalen Spezifikation und dem High-Level Entwurf
- Analyse der Übereinstimmung zwischen dem High-Level- und Low-Level-Entwurf
- Analyse der Übereinstimmung zwischen dem Low-Level-Entwurf und der Darstellung der Implementation
- Analyse der Übereinstimmung zwischen dem Low-Level-Entwurf und Teile der Implementationsdarstellung
- Übergabeprotokoll
- Übergabe-Verfahren einschließlich der Aufnahme in Verfahrenshandbücher
- Deskriptive Darstellung vom Low-Level-Entwurf
- Formales Sicherheitsmodell des Produktes
- Definition des Lebenszyklus
- Abdeckungsanalyse für Testberichte
- Test-Dokumentation
- Das Produktmodell für Sicherheitspolicy

T4: Optionale Dokumente, die der Hersteller freiwillig bereitstellen kann

- Dokumentation der Sicherheit während der Entwicklung
- Dokumentation der Entwicklungstools
- Low-Level-Entwurf (*Threads, IPC, Memory Management*, etc.)
- Analyse der Mißbrauchsmöglichkeiten der mit dem Produkt mitgelieferten Dokumentation

- Nachweis der Abdeckung der Testberichte
- Analyse der Tiefe der Testberichte
- Quellcode

Je mehr aktuelle und relevante Dokumente dem Sachverständigen zur Verfügung gestellt werden, desto effizienter und kostengünstiger das Verfahren! Die Verwendung von qualitätsgesicherten Entwicklungstools und –verfahren sowie die bereits bei der Entwicklung des Produktes ab initio beachtete Ausrichtung auf Datenschutz reduzieren in der Regel die notwendige Prüftiefe.

Grenzen der Produktdokumentation

Auch wenn die Produktdokumentationen in der Zertifizierungsvorbereitung die Hauptrolle spielen, soll ihre Bedeutung nicht überschätzt werden. Daher soll auf folgende Tatsachen hingewiesen werden:

- Für Softwaredokumentation wird i.d.R. kein Standard eingesetzt, deswegen ist es sehr schwierig, zwei Produkte nur anhand ihrer Dokumentation zu vergleichen.
- Entsprechend kann es keine allgemeingültige Methode zur Analyse der Dokumentation geben.
- Es ist aufwendig nachzuweisen, dass die in der Dokumentation beschriebenen Funktionen auch tatsächlich *richtig* und *vollständig* implementiert sind.
- In vielen Fällen sind die erforderlichen Pflicht-Dokumente einfach nicht vorhanden! Bei fehlender Dokumentation muss der Sachverständiger durch direkte Anfrage die erforderlichen Informationen vom Hersteller nachholen.
- Die „Reparatur“ von technischen Mängeln durch Verfahrens-anweisungen findet ihre Grenze in der teilweise hohen Komplexität und der Nutzerakzeptanz solcher Maßnahmen. Es wird hier auf die Hinweise zur Bewertung in der Publikation „Das schleswig-holsteinische Datenschutzgütesiegel“, Stand: 2002-02-01, V 1.0 verwiesen: Sind die organisatorischen Maßnahmen zur Reparatur unzumutbar, gilt die Anforderung als nicht erfüllt. Eine Siegelerteilung ist in einem solchen Fall ausgeschlossen.

Glossar

Dokumentation von Schwachstellen:

Unstrukturierte Zusammenstellung von Hinweisen auf nicht erwartungsgemäßes Verhalten des Produktes, ggfs. auch aus Fremdquellen (z.B. Pressemitteilung über Probleme bei einem Basissystem).

Risikoanalyse:

Strukturierte Dokumentation und Bewertung von produktinherenten Risiken sowie möglicher Abilfemaßnahmen (Workarounds).

Schwachstellenanalyse

Strukturierte Dokumentation und Bewertung von produktinherenten und sich aus der Einsatzumgebung ergebenden Risiken sowie möglicher Abhilfemaßnahmen (Workarounds).

---

[i] T1 wurde in den bislang veröffentlichten Papieren auch als „Beipackzettel“ bezeichnet.

[ii] Z.B., kann eine Schwachstellenanalyse für ein spezialisiertes Netzgerät wie einen Router als Pflicht-Dokumentation betrachtet werden, während sie für eine Software nicht immer sinnvoll ist.

[iii] Als Beispiel kann der Unterschied zwischen einem herkömmlichen Office-Paket und ein Warenwirtschaftsystem (WWS) erwähnt werden. Sie unterscheiden sich u.a. dadurch, dass ein WWS i.d.R. eine erhebliche Anpassungsarbeit (Implementierung und Customizing) voraussetzt. Deshalb ist für ein WWS ein Übergabeprotokoll ein Pflicht-Dokument, während bei dem Office-Paket ein Übergabeprotokoll schon in Form eines Lieferschein ausreichend sein kann.