APP: Anwendungen

APP.7: Entwicklung von Individualsoftware

1 Beschreibung

1.1 Einleitung

Viele Institutionen stehen vor Herausforderungen, die sie nicht mehr hinreichend mit unangepasster Software lösen können. Die mit diesen Herausforderungen verbundenen Aufgabenstellungen bedürfen häufig Softwarelösungen, die auf die individuellen Bedürfnisse der Institutionen zugeschnitten sind. Im Folgenden werden diese Softwarelösungen als Individualsoftware bezeichnet. Hierzu können einerseits Basislösungen, die aus einer Grundmenge an typischen Funktionen bestehen, eingesetzt und individualisiert werden. Die Grundfunktionen werden hierbei für den individuellen Einsatzzweck der Institution angepasst und um individuell benötigte Funktionen erweitert. Gängige Beispiele hierfür sind IT-Anwendungen wie ERP- (Enterprise Resource Planning), CMS- (Content Management Systeme) oder IDM-Systeme (Identity Management). Individualsoftware kann auch vollständig neu von der Institution selbst oder von Dritten entwickelt werden. Hierzu gehören Anwendungen zur Geschäftsprozesssteuerung oder individuell angepasste Fachanwendungen, wie Personalverwaltungssoftware, Verfahren zur Verwaltung von Sozialdaten oder Meldedaten.

Von essentieller Bedeutung ist es hierbei, dass bereits bei der Planung und Konzeptionierung der Individualsoftware auch die benötigten Sicherheitsfunktionen bedacht werden und die Informationssicherheit in dem gesamten Lebenszyklus der Individualsoftware berücksichtigt wird. Fehler in der Planung oder fehlende Sicherheitsfunktionen können im laufenden Betrieb nicht oder nur mit hohem zusätzlichen Aufwand ausgeglichen werden.

Individualsoftware wird dabei in der Regel im Rahmen eines Projektes entwickelt. Hierzu haben sich die unterschiedlichsten Vorgehens- bzw. Projektmanagementmodelle etabliert. Während klassische, lineare Vorgehensmodelle, wie der Wasserfallprozess, sehr gut zu Projekten mit zu Beginn feststehenden Anforderungen passen, ermöglichen agile Vorgehensmodelle, wie Scrum, Individualsoftware iterativ und inkrementell zu entwickeln. Agile Vorgehensmodell können sich somit besser an verändernde Gegebenheiten anpassen, insbesondere wenn zu Beginn noch nicht alle Anforderungen feststehen. Allerdings bieten sie nicht die selbe Kalkulationssicherheit wie lineare Vorgehensmodelle und passen auch in einigen Fällen nicht zu den klassischen Strukturen der Beschaffungsprozesse, die auf ein lineares Vorgehen ausgerichtet sind.

1.2 Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, welche grundlegenden Sicherheitsanforderungen bei der Planung und Entwicklung von Individualsoftware zu berücksichtigen sind.

1.3 Abgrenzung und Modellierung

Der Baustein APP.7 *Entwicklung von Individualsoftware* ist für jede Entwicklung einer Individualsoftware einmal anzuwenden.

Aspekte zur Planung, Konzeption und Einsatz von Individualsoftware, wie benötigte Sicherheitsfunktionen festzulegen oder Individualsoftware außer Betrieb zu nehmen, werden im Baustein APP.6 *Auswahl und Einsatz von Software* behandelt. Er ist daher immer zusammen mit diesem Baustein anzuwenden.

Wenn Software entwickelt wird, liegt sehr häufig ein Auftragnehmer und Auftraggeber-Verhältnis vor. Im IT-Grundschutz spiegelt sich dieser Sachverhalt wider, indem der Baustein APP.7 *Entwicklung von Individualsoftware* die Auftragsgeberseite und der Baustein CON.8 *Software-Entwicklung* die Auftragnehmerseite behandeln.

Die Freigabe und Tests von Individualsoftware wird im Baustein OPS.1.1.6. *Software-Tests und -Freigaben* behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.7 *Entwicklung von Individualsoftware* von besonderer Bedeutung.

2.1 Unzulängliche vertragliche Regelungen mit externen Dienstleistern

Aufgrund von unzulänglichen vertraglichen Regelungen mit externen Dienstleistern können vielfältige und schwerwiegende Sicherheitsprobleme auftreten. Dies gilt insbesondere, wenn Anwendungen erstellt, eingeführt oder gewartet werden. Sind Aufgaben, Leistungsparameter oder der Aufwand ungenügend oder missverständlich beschrieben, können Sicherheitsmaßnahmen möglicherweise aus Unkenntnis oder aufgrund mangelnder Qualifizierung oder fehlender Ressourcen nicht umgesetzt werden. Dies kann viele negative Auswirkungen nach sich ziehen, etwa wenn regulatorische Anforderungen und Pflichten nicht erfüllt werden, Auskunftspflichten und Gesetze nicht eingehalten werden oder keine Verantwortung übernommen wird, weil Kontroll- und Steuerungsmöglichkeiten fehlen.

2.2 Software-Konzeptionsfehler

Werden Anwendungen, Programme und Protokolle konzeptioniert, können sicherheitsrelevante Konzeptionsfehler entstehen. Diese ergeben sich häufig daraus, dass Anwendungsmodule und Protokolle, die für einen bestimmten Zweck vorgesehen sind, in anderen Einsatzszenarien wiederverwendet werden. Sind dann andere Sicherheitsvorgaben relevant, kann dies zu massiven Sicherheitsproblemen führen, zum Beispiel wenn Anwendungsmodule und Protokolle, die eigentlich für abgeschottete betriebliche Umgebungen vorgesehen sind, an das Internet angebunden werden.

2.3 Undokumentierte Funktionen

Viele Anwendungen enthalten vom Hersteller eingebaute, undokumentierte Funktionen, häufig für die Entwicklung oder zum Support der Anwendung. Diese sind den Benutzern meistens nicht bekannt. Undokumentierte Funktionen sind dann problematisch, wenn sie es erlauben, dass wesentliche Sicherheitsmechanismen umgangen werden, z. B. zum Zugriffsschutz. Dies kann die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten erheblich beeinträchtigen.

2.4 Fehlende oder unzureichende Sicherheitsmaßnahmen in Anwendungen

Sicherheitsmechanismen oder Sicherheitsfunktionen sollen in der Anwendung sicherstellen, dass bei der Verarbeitung von Informationen die Vertraulichkeit, Integrität und Verfügbarkeit im benötigten Maße gewährleistet werden können. Häufig steht bei der Entwicklung einer Anwendung aber die fachliche Funktionalität oder der Zeit- und Kostenrahmen im Vordergrund. So können wichtige Sicherheitsmechanismen zu schwach ausgeprägt sein, sodass sie einfach umgangen werden können oder sogar ganz fehlen.

2.5 Mangelhafte Steuerung der Software-Entwicklung

Wird die Software-Entwicklung vom Auftraggeber nicht hinreichend gesteuert, bestehen eine Reihe von Gefahren, wie z.B.:

- Es können geforderte Sicherheitsfunktionen fehlen oder nur unzureichend implementiert werden. Hieraus können sich vielfältige Risiken ergeben, die die Verfügbarkeit, Vertraulichkeit und Integrität der mit der Individualsoftware verarbeiteten Daten gefährden.
- Das Entwicklungsprojekt kann sich zeitlich verzögern, sodass die Individualsoftware nicht rechtzeitig verfügbar ist.
- Prioritäten können falsch gesetzt werden, indem z.B. nachrangig benötigte Funktionen umfangreich entwickelt werden und dringend benötigte Sicherheitsfunktionen nur rudimentär implementiert werden. Auch hieraus können Projektverzögerungen und vielseitige Sicherheitsrisiken entstehen.

2.6 Beauftragung ungeeigneter Software-Entwickler

Werden ungeeignete Software-Entwickler beauftragt, können daraus unterschiedliche Gefährdungen entstehen:

- Aufgrund fehlender fachlicher Expertise, z.B. in der verwendeten Programmiersprache, in den eingesetzten Frameworks oder der geplanten technischen Einsatzumgebung, kann die Software viele vermeidbare Sicherheitslücken umfassen.
- Fehlende Kenntnisse im Bereich des Projektmanagements und Requirements Engineering können zu Reibungsverlusten in Abstimmungsprozessen und somit zu erheblichen Verzögerungen führen. Auch können deswegen Schwerpunkte falsch gesetzt werden und so wesentliche Sicherheitsfunktionen nicht mit der erforderlichen Priorität implementiert werden.Ungeeignete Software-Entwickler können beispielsweise aufgrund zu knapper, unrealistischer Kostenkalkulationen beauftragt werden. Auch Fehler, missverständliche Anforderungen und falsche Zielvorstellungen in Ausschreibungen können dazu führen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.7 *Entwicklung von Individualsoftware* aufgeführt. Grundsätzlich ist der Fachverantwortliche für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Fachverantwortliche

Weitere Zuständigkeiten	Beschaffungsstelle, IT-Betrieb

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.7 *Entwicklung von Individualsoftware* vorrangig erfüllt werden:

APP.7.A1 Erweiterung der Planung des Software-Einsatzes um Aspekte von Individualsoftware (B)

Die Planung des Software-Einsatzes MUSS um Aspekte von Individualsoftware ergänzt werden, indem definiert wird,

- wer dafür zuständig ist, die Software-Entwicklung bzw. den Auftragnehmer zu steuern und zu koordinieren, sowie
- in was für einen organisatorischen Rahmen die Software zu entwickeln ist (Projektmanagementmodell)

Individualsoftware SOLLTE im Rahmen eines Entwicklungsprojektes entwickelt werden. Das Entwicklungsprojekt sollte anhand eines Ablaufplans zeitlich grob geplant werden.

APP.7.A2 Festlegung von Sicherheitsanforderungen an den Prozess der Software-Entwicklung (B)

Die Institution MUSS klare Anforderungen an den Prozess der Software-Entwicklung definieren. Aus den Anforderungen MUSS hervorgehen, in was für einer Umgebung die Software entwickelt werden darf und welche technischen und organisatorischen Maßnahmen von Seiten der beauftragten Software-Entwickler umzusetzen sind.

APP.7.A3 Festlegung der Sicherheitsfunktionen zur System-Integration [IT-Betrieb] (B)

Der IT-Betrieb und die zuständigen Fachverantwortlichen MÜSSEN Anforderungen an die technische Einsatzumgebung der geplanten Individualsoftware erstellen und mit der Software-Entwicklung abstimmen. Aus den Anforderungen MUSS klar hervorgehen:

- auf was für einer Hardware-Plattform,
- auf was für einer Software-Plattform (inklusive gesamten Software-Stack),
- mit welchen zur Verfügung stehenden Ressourcen (z.B. CPU-Cluster oder Arbeitsspeicher),
- mit welchen Schnittstellen mit anderen Systemen sowie
- mit welchen sich hieraus ergebenen Sicherheitsfunktionen

die Anwendung eingesetzt werden soll. Schnittstellen mit anderen IT-Systemen SOLLTEN in standardisierten technischen Formaten modelliert und definiert werden.

APP.7.A4 Anforderungsgerechte Beauftragung [Beschaffungsstelle] (B)

Wird Individualsoftware durch die eigene Institution entwickelt oder extern beauftragt, dann MÜSSEN neben den bestehenden rechtlichen und organisatorischen Vorgaben insbesondere

- der Anforderungskatalog (siehe hierzu APP.6 *Allgemeine Software*),
- die Sicherheitsanforderungen an den Prozess der Software-Entwicklung, sowie
- die Sicherheitsfunktionen zur System-Integration

als Grundlage zur Software-Entwicklung verwendet werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.7 *Entwicklung von Individualsoftware*. Sie SOLLTEN grundsätzlich erfüllt

werden.

APP.7.A5 Geeignete Steuerung der Anwendungsentwicklung (S)

Bei der Entwicklung von Individualsoftware SOLLTE ein geeignetes Steuerungs- und Projektmanagementmodell verwendet werden. Hierbei SOLLTE das ausgewählte Modell mit dem Auftragnehmer abgestimmt werden. Bei der Steuerung SOLLTE es berücksichtigt werden.

Es SOLLTE insbesondere berücksichtigt werden, dass das benötigte Personal ausreichend qualifiziert ist. Alle relevanten Phasen SOLLTEN während des Lebenszyklus der Software abgedeckt werden. Außerdem SOLLTE es ein geeignetes Entwicklungsmodell, ein Risikomanagement sowie Qualitätsziele enthalten.

APP.7.A6 Dokumentation der Anforderungen an die Individualsoftware (S)

Die Anforderungen aus den Anforderungskatalog, die Sicherheitsanforderungen an den Prozess der Software-Entwicklung, sowie die Sicherheitsfunktionen zur System-Integration SOLLTEN umfassend dokumentiert werden. Insbesondere SOLLTE ein Sicherheitsprofil für die Anwendung erstellt werden. Dieses SOLLTE den Schutzbedarf der zu verarbeiteten Daten und Funktionen dokumentieren. Die Dokumentation mitsamt Sicherheitsprofil SOLLTE den Entwicklern zur Software-Entwicklung zur Verfügung gestellt werden.

Die Dokumentation SOLLTE bei Änderungen an der Individualsoftware sowie bei funktionalen Updates aktualisiert werden.

APP.7.A7 Sichere Beschaffung von Individualsoftware (S)

Das Entwicklungsprojekt SOLLTE im Rahmen des hierfür bestens geeigneten Projektmanagementmodells beauftragt werden. Sicherheitsaspekte SOLLTEN dabei bereits bei der Ausschreibung und Vergabe berücksichtigt werden, sodass

- einerseits nur geeignete Auftragnehmer beauftragt werden,
- andererseits aber keine weitreichenden Rückschlüsse auf die Sicherheitsarchitektur durch die öffentlich verfügbaren Informationen möglich sind.

In der Institution SOLLTEN definierte Prozesse und festgelegte Ansprechpartner existieren, die sicherstellen, dass die jeweiligen Rahmenbedingungen berücksichtigt werden.

APP.7.A8 Frühzeitige Beteiligung des Fachverantwortlichen bei entwicklungsbegleitenden Software-Tests (S)

Der Fachverantwortliche SOLLTE schon vor der endgültigen Abnahme frühzeitig an entwicklungsbegleitenden Tests der Softwareentwickler beteiligt werden. Dies SOLLTE in Abstimmung mit dem Auftragnehmer bereits initial im Projektablaufplan berücksichtigt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.7 *Entwicklung von Individualsoftware* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.7.A9 Treuhänderische Hinterlegung (H)

Für institutionskritische Anwendungen SOLLTE geprüft werden, ob diese gegen Ausfall des Herstellers abgesichert werden. Dafür SOLLTEN nicht zum Lieferumfang der Anwendung gehörende Materialien und Informationen treuhänderisch hinterlegt werden, etwa bei einer Escrow-Agentur. Dokumentierter Code, Konstruktionspläne, Schlüssel oder Passwörter SOLLTEN dazu gehören. Die Pflichten der Escrow-Agentur zur Hinterlegung und Herausgabe SOLLTEN vertraglich geregelt werden. Es SOLLTE geklärt werden, wann das Hinterlegte an wen herausgegeben werden darf.

APP.7.A10 Beauftragung zertifizierter Software-Entwicklungsunternehmen (H)

Werden besonders sicherheitskritische Anwendungen entwickelt, SOLLTEN hierzu zertifizierte Software-Entwickler beauftragt werden. Die Zertifizierung SOLLTE Sicherheitsaspekte für relevante Aspekte der Software-Entwicklung umfassen.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt

- in der Norm ISO/IEC 12207:2008, „System and software engineering - Software life cycle process“ einen Überblick über alle Bestandteile des Lebenszyklus einer Software,
- in der Norm ISO/IEC 15408-2:2008, „Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components“ einen Überblick über die Möglichkeiten der Systemabsicherung und
- in der Norm ISO/IEC 27001:2013, „Information technology - Security technigues - Information security management systems – Requirements“ im Annex A, A.14 System acquisition, development and maintenance“ Anforderungen an die System-Entwicklung und den -betrieb.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in der „Area BA Business Application Management“ Anforderungen an das Management von Business-Anwendungen.

Das National Institute of Standards and Technology stellt in der „NIST Special Publication 800-53“ im Apendix F-SA „Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity“ weitergehende Anforderungen an den Umgang mit Individualsoftware.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.7 *Entwicklung von Individualsoftware* von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.45 Datenverlust