Informationssicherheits-Navigator

„Best Practice“-Ansätze zur Entwicklung sicherer Software

V-Modell XT Bund (Version: 2.3)

In diesem Dokument werden wesentliche Ansätze zur Verbesserung der Informationssicherheit bei der Entwicklung von Software-Systemen angesprochen, die an verschiedenen Stellen im V-Modell XT Bund enthalten sind. Dieses Dokument soll die Aufmerksamkeit auf diese „Best-Practice“-Ansätze lenken und deren Auffinden im V-Modell-Kontext erleichtern.

Nutzen Sie dieses Dokument als „Informationssicherheits-Navigator“ im V-Modell XT Bund.

1 Prinzipien

1.1 Relevanz

Frühe Entscheidungen sind später meist nur mit viel Aufwand zu revidieren. Prüfen Sie als Auftraggeber daher **bereits vor Beginn eines Projekts**, ob Informationssicherheit und Datenschutz in Ihrem Vorhaben von Bedeutung sind. Nutzen Sie dazu die Checkliste Informationssicherheit und berücksichtigen das Ergebnis in Ihrem weiteren Vorgehen. Holen Sie im Zweifel eine zweite Meinung ein.

Fundstelle im V-Modell XT Bund: C.1.1.2 Checkliste Informationssicherheit

1.2 Vorgaben

Informationssicherheit und Datenschutz lassen sich nicht nachträglich in ein System „hineintesten“, sondern müssen von Anfang an als wichtige Ziele eines sicherheitskritischen IT-Projekts verfolgt werden. Verschaffen Sie sich als Auftraggeber zum Projektbeginn einen Überblick über die in Ihrer Behörde geltenden Vorgaben zur Informationssicherheit, zum Datenschutz und zum IT-Betrieb. Berücksichtigen sie diese in Ihrem Projekt und fordern vom Auftragnehmer deren Beachtung ein.

Fundstelle im V-Modell XT Bund: C.1.10.2 Vorgaben zur Informationssicherheit, C.1.10.3 Vorgaben zum Datenschutz, C.1.15.1 Vorgaben zum IT-Betrieb

1.3 Kontinuierliche Verbesserung

Geben Sie als Auftraggeber die in Ihrem Projekt gewonnenen Erkenntnisse weiter, um die vorgenannten Vorgaben mit neuem Wissen anzureichern. Fordern Sie vom Auftragnehmer Erweiterungen der Vorgaben ein, die die im Projekt hinzugekommenen Anforderungen an die Informationssicherheit, den Datenschutz und den IT-Betrieb abdecken.

Fundstelle im V-Modell XT Bund: C.1.11.7 Erweiterung der Vorgaben zur Informationssicherheit, C.1.11.8 Erweiterung der Vorgaben zum Datenschutz, C.1.15.2 Erweiterung der Vorgaben zum IT-Betrieb

2 Projektorganisation und -umgebung

2.1 Personal

Binden Sie Sicherheitsexperten in Ihr Projekt ein! Nutzen Sie das Wissen des Informationssicherheits- und des Datenschutzbeauftragten Ihrer Organisation. Sorgen Sie dafür, dass Ihr Projektteam über einen Informationssicherheitsverantwortlichen mit langjähriger Erfahrung und breiter Expertise im notwendigen Umfang verfügen kann.

Fundstelle im V-Modell XT Bund: D.3.2 Datenschutzbeauftragter, D.3.4 Informationssicherheitsbeauftragter, D.1.7 Datenschutzverantwortlicher, D.1.9 Informationssicherheitsverantwortlicher

2.2 Schulungen

Schicken Sie Ihre Projektmitarbeiter auf Schulungen zu Informationssicherheit und Datenschutz, um sie mit den nötigen Kenntnissen auszustatten und für entsprechende Risiken zu sensibilisieren. Sorgen Sie als Auftragnehmer dafür, dass Ihre Entwickler Bug Patterns kennen und ihnen grobe Schnitzer à la OWASP Top Ten nicht unterlaufen.

Fundstelle im V-Modell XT Bund: Mustertexte für die Produktvorlagen Projekthandbuch (Organisation und Vorgaben zu Informationssicherheit und Datenschutz, Organisation und Vorgaben zur Systemerstellung, Vorgaben für das Projekthandbuch der Auftragnehmer), Implementierungs-, Integrations- und Prüfkonzept SW (Vorgehen zur Realisierung und Realisierungsumgebung)

2.3 Werkzeuge

Wählen Sie die im Projekt benötigten Werkzeuge zur Planung, Verwaltung, Kommunikation und Entwicklung auch nach Aspekten der Informationssicherheit aus. Unterstellen Sie die Werkzeuge Ihres Projekts dem Informationssicherheits-Managementsystem (ISMS) Ihrer Organisation.

Fundstelle im V-Modell XT Bund: C.1.1.5.14 Organisation und Vorgaben zum Informationssicherheits-Managementsystem

2.4 Zugriff

Gewähren Sie nur solchen Personen Zugriff auf Projektdaten und -ergebnisse, die diesen auch benötigen („Need-to-Know“). Dadurch verringern Sie unter anderem das Risiko, dass Hintertüren in Software eingebaut, vertrauliche Informationen weitergegeben oder geheime Schlüssel Unbefugten zugänglich gemacht werden.

Fundstelle im V-Modell XT Bund: C.1.5.1 Produktbibliothek, C.1.11.5.1 Vorgehen zur Realisierung und Realisierungsumgebung, C.1.16.2.1 Kriterien zur Gewährleistung der Informationssicherheit und des Datenschutzes

3 Lastenheft

3.1 Sicherheits-Anforderungen

Integrieren Sie als Auftraggeber die Vorgaben zu Informationssicherheit, Datenschutz und IT-Betrieb (siehe 1.2) als Anforderungen in das Lastenheft oder die Ausschreibungsunterlagen, damit sie im zu entwickelnden System eingehalten bzw. umgesetzt werden.

Fundstelle im V-Modell XT Bund: C.1.10.1.3 Nicht-Funktionale Anforderungen

3.2 Schutzbedarf

Stellen Sie als Auftraggeber für das zu entwickelnde System und die von ihm verarbeiteten Informationen fest, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit haben. Orientieren Sie sich dabei an den möglichen Schäden und Folgen für Betroffene, die eine Verletzung der Schutzziele verursachen würde. Integrieren Sie die Schutzbedarfsfeststellung in das Lastenheft oder in Ihre Ausschreibungsunterlagen, um dem Auftragnehmer die Erarbeitung einer zielgerichteten Sicherheitskonzeption zu ermöglichen. Passen Sie die Schutzbedarfsfeststellung im Dialog mit dem Auftragnehmer kontinuierlich an neue Erkenntnisse aus dem Projektverlauf an.

Fundstelle im V-Modell XT Bund: C.1.10.5 Schutzbedarfsfeststellung, C.1.10.1.3 Nicht-Funktionale Anforderungen, C.1.11.6 Sicherheitskonzeption

4 Systementwurf

4.1 Sicherheitskonzeption

Erstellen Sie als Auftragnehmer eine Sicherheitskonzeption, in der Sie die Risiken für die Informationssicherheit und den Datenschutz systematisch identifizieren, abschätzen und mit passenden Maßnahmen behandeln. Der Informationssicherheitsverantwortliche stellt sicher, dass die Sicherheitskonzeption in jeder Iteration verfeinert wird und ihre Inhalte in die Spezifikation der zu entwickelnden Systemelemente eingehen. Er sichert deren Umsetzung im späteren Projektverlauf durch entsprechende Tests ab und sorgt zudem dafür, dass zusätzlich identifizierte Anforderungen in die Erweiterungen der Vorgaben des Auftraggebers zu Informationssicherheit, Datenschutz oder IT-Betrieb (siehe 1.3) einfließen.

Diskutieren Sie als Auftraggeber mit dem Auftragnehmer verbleibende Restrisiken. Wägen Sie ab, welche der Restrisiken Sie zu tragen bereit sind, und treffen Sie eine entsprechende Vereinbarung mit dem Auftragnehmer. Beziehen Sie den Informationssicherheitsbeauftragten Ihrer Behörde und des künftigen Betreibers in die Entscheidung mit ein und sorgen Sie für den Rückfluss der Erkenntnisse in Ihre Behörde (siehe 1.3).

Fundstelle im V-Modell XT Bund: C.1.11.6 Sicherheitskonzeption, D.1.9 Informationssicherheitsverantwortlicher, D.3.4 Informationssicherheitsbeauftragter, C.1.11.6.8 Risikoabschätzung, Risikobehandlung und Restrisiken

4.2 Designprinzipien

Verwenden Sie als Auftragnehmer etablierte Designprinzipien für die Entwicklung sicherer Softwaresysteme. Orientieren Sie sich dabei beispielsweise an den Anforderungen aus den Bausteinen Softwareentwicklung, Software-Tests und -Freigaben, Entwicklung und Einsatz von Fachanwendungen des IT-Grundschutz-Kompendiums des BSI.

Fundstelle im V-Modell XT Bund: Mustertexte für die Produktvorlage Projekthandbuch (Organisation und Vorgaben zur Systemerstellung)

4.3 Einsatz von Kryptografie

Setzen Sie als Auftragnehmer kryptografische Verfahren wie Verschlüsselung, Checksummen oder digitale Signaturen nach dem Stand der Technik ein. Nutzen Sie dazu beispielsweise das öffentlich verfügbare Expertenwissen des BSI und dessen Empfehlungen zur Auswahl geeigneter kryptografischer Verfahren und deren optimaler Parametrisierung. Verwenden Sie vorhandene Verfahren und entwickeln Sie keine eigenen kryptografischen Lösungen.

Fundstelle im V-Modell XT Bund: C.1.10.2 Vorgaben zur Informationssicherheit, C.1.10.3 Vorgaben zum Datenschutz, C.1.11.5.1 Vorgehen zur Realisierung und Realisierungsumgebung

5 Implementierung

5.1 Coding Standards

Legen Sie als Auftragnehmer Programmiervorgaben zur Erstellung sicherer Software wie die SEI Cert Coding Standards fest und achten Sie auf deren Einhaltung. Schließen Sie dadurch leicht vermeidbare Fehler im Rahmen der Programmierung weitgehend aus.

Fundstelle im V-Modell XT Bund: Mustertexte für die Produktvorlage Projekthandbuch (Organisation und Vorgaben zur Systemerstellung)

5.2 Verwendung externer Komponenten

Schränken Sie als Auftragnehmer die Verwendung externer Komponenten (Externe Software-Produkte) auf solche ein, die hinsichtlich der Informationssicherheit und des Datenschutzes von Ihnen oder vertrauenswürdigen Dritten geprüft wurden. Verwenden Sie nach Möglichkeit Komponenten mit offengelegtem Quellcode. Reduzieren Sie die externen Komponenten soweit möglich auf das für das Projekt notwendige Maß an Funktionalität. Dokumentieren Sie die verwendeten Komponenten über entsprechende Automatismen (z. B.: License Maven Plugin).

Fundstelle im V-Modell XT Bund: C.1.11.2.2 Dekomposition des Systems, C.1.11.2.3 Externe Systemelemente, C.1.11.3.2 Dekomposition der SW-Einheit, C.1.11.3.3 Externe SW-Elemente

6 Test

Stellen Sie als Auftragnehmer sicher, dass die Maßnahmen zur Umsetzung von Informationssicherheits-Anforderungen greifen. Prüfen Sie daher deren Umsetzung analog zur Umsetzung fachlicher Anforderungen durch entsprechende Testroutinen.

Fordern Sie als Auftraggeber vom Auftragnehmer die Lieferung des Testkonzepts, der Testfälle und -routinen sowie der Konfiguration von Testwerkzeugen und übergeben Sie dies an den Verfahrensverantwortlichen zur Absicherung des Betriebs und der Weiterentwicklung des Systems.

Fundstelle im V-Modell XT Bund: C.1.6.9.6 Prüfkriterien für die Systemdokumentation, C.1.16.2.1 Kriterien zur Gewährleistung der Informationssicherheit und des Datenschutzes, Mustertexte für die Produktvorlagen Projekthandbuch (Organisation und Vorgaben zur Systemerstellung), QS-Handbuch (Vorgaben für das QS-Handbuch der Auftragnehmer)

6.1 Dynamisches Testen

Führen Sie regelmäßig automatisierte Tests des laufenden Systems zum Auffinden typischer Schwachstellen mit geeigneten Werkzeugen (z.B. Fuzzing) durch. Schwachstellen dieser Art sind für Angreifer, die die gängigen Werkzeuge ebenfalls nutzen, besonders leicht aufzufinden und auszunutzen und müssen daher unbedingt beseitigt werden.

Validieren Sie Informationssicherheitsmaßnahmen, die für die Verringerung hoher Risiken maßgeblich sind, und den Schutz besonders wichtiger Bestandteile des Systems (mit hohem oder sehr hohem Schutzbedarf) durch Penetrationstests.

6.2 Statisches Testen

Sehen Sie statische Tests vor, die neben den funktionalen Aspekten der Informationssicherheitsmaßnahmen auch die Sicherheitseigenschaften des Systemelements validieren sollen. Dies umfasst unter anderem:

6.2.1 Regelmäßige Reviews / Audits

Prüfen Sie regelmäßig durch Reviews und Audits die Qualität des Quellcodes Ihrer selbst erstellten Komponenten und der externen Komponenten mit offengelegtem Quellcode. Beteiligen Sie Informationssicherheitsexperten, die Schwachstellen im Quellcode erkennen können.

6.2.2 Einhaltung der Design- und Coding-Vorgaben

Prüfen Sie den Quellcode Ihrer selbst erstellten Komponenten regelmäßig mit geeigneten Werkzeugen auf die Einhaltung der Design-Vorgaben und der gewählten Coding Standards (siehe 5.1).

Prüfen Sie auch die externen Komponenten mit offengelegtem Quellcode gegen Ihre Design-Vorgaben. Abweichungen können Hinweise auf Schwächen externer Komponenten, aber auch auf Nachteile eigener Vorgaben sein.