Wie Vertrauen in kritische Software geschaffen werden kann

Immer mehr Software steuert relevante Aufgaben im Finanzwesen, im Gesundheitswesen, in der Energieversorgung und natürlich in allen anderen Lebensbereichen. Wir müssen dieser Software vertrauen und mit einer gewissen Sicherheit sagen können, dass sie das tut, was wir von ihr erwarten.

Kay Grosskop, Pascal Sieber

Dieses Vertrauen können wir unter anderem aufbauen, indem wir Software analysieren und zertifizieren. Damit dies möglich ist, muss die Software gewissen Anforderungen an die Auditierbarkeit genügen, denn was nicht analysiert werden kann, kann auch nicht verstanden und damit nicht gemessen werden.

Auditability Assessment Model

Software wird heute eingesetzt, um sehr sensible und kritische Prozesse mit ebenso sensiblen Daten zu unterstützen oder zu digitalisieren. Nur wenn der Code auditierbar ist, kann überprüft werden, was die Software tut, wie sie mit bestimmten Daten umgeht, wie sie bestimmte Daten schützt und wie sichergestellt wird, dass keine Manipulation durch Dritte stattfinden kann. Ein übliches Vorgehen ist die Analyse des Softwarecodes. Dieser blosse Zugriff auf den Quellcode reicht aber nicht aus. Wenn der Code komplex geschrieben, schlecht dokumentiert und unvollständig ist, kann er schwer oder gar nicht geprüft werden. Die Folge davon: Nur noch wenige Insider haben überhaupt eine Chance zu verstehen, wo die Risiken liegen, und deren Urteil ist subjektiv, kann also vom Management und der Öffentlichkeit nicht nachvollzogen werden. Nachvollziehbarkeit bedeutet, dass eine Person mit entsprechenden Vorkenntnissen innerhalb einer angemessenen Zeit verstehen kann, was genau im Code passiert. Wir abstrahieren diese Anforderung, sodass sie auf jede Software in jeder Technologie anwendbar ist, in drei Aspekte (vgl. Abbildung 1):

Produktqualität

Der Kern des Aspekts «Produktqualität» ist die Frage der Wartbarkeit. Warum ist die Wartbarkeit ein Aspekt der Auditierbarkeit? Ein Prüfer muss verstehen, was die Software tut, wie Funktionen implementiert werden und wie bestimmte Teile des Codes mit anderen verbunden sind. Dies sind auch Aufgaben, die bei der normalen Wartung von Software durch einen Entwickler anfallen. Wenn der Code gewartet werden muss, d. h. wenn Änderungen am Code vorgenommen werden, muss der Entwickler schnell verstehen, was dieser Teil des Codes tut. Er ist also mit den gleichen Anforderungen konfrontiert wie ein Auditor. Einige Aspekte, die nicht durch das Modell der Wartbarkeit abgedeckt werden, sind ebenfalls enthalten. Zum Beispiel die Wahl der Technologie. Wird ein Technologie-Stack oder eine Plattform verwendet, die weit verbreitet und gut bekannt ist? Oder wird eine exotische Plattform gewählt, in die sich ein potenzieller Prüfer erst einarbeiten muss, um zu verstehen, was genau im Code passiert?

Dokumentation

Die Dokumentation ist ein wesentliches Mittel, um eine Codebasis zu verstehen. Diese Informationen aus Reverse Engineering oder Interviews zu extrahieren, erschwert den Audit-Prozess erheblich. Testautomatisierungsskripte, Funktionsdokumentation oder Installations- und Betriebsanweisungen tragen ebenfalls zum Verständnis der Funktionsweise der Software bei. Bei der Bewertung liegt der Schwerpunkt hier auf Vollständigkeit, Qualität und Aktualität.

Veröffentlichbarkeit

Wenn bisher unveröffentlichte Software öffentlich gemacht wird, gibt es bestimmte Bereiche, die besondere Aufmerksamkeit erfordern. Andernfalls kann die Software nicht vollständig oder nur von einem ausgewählten Kreis von autorisierten Gutachtern überprüft werden. Unter dem Aspekt der Publizierbarkeit wird geprüft, inwieweit auf Code-Ebene die Voraussetzung für eine Veröffentlichung bzw. eine umfassende Prüfung des Codes gegeben ist. Enthält der Code z. B. noch vertrauliche Informationen, die datenschutzrechtlich relevant sein könnten, wie

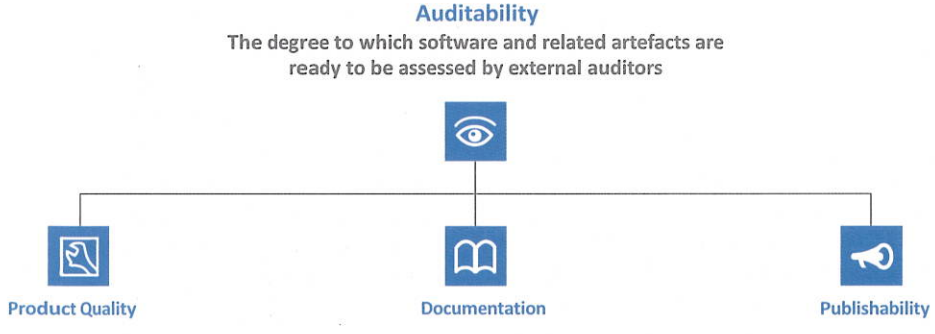

Abbildung 1: Aspekte der Auditierbarkeit

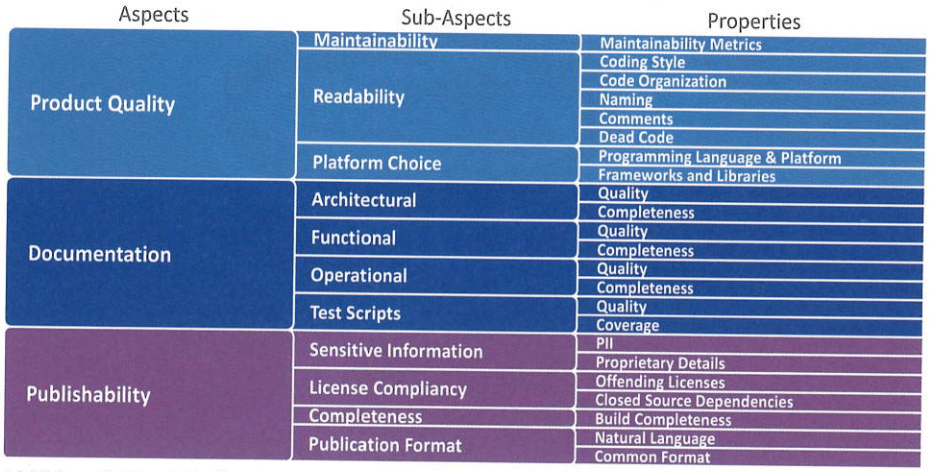

Abbildung 2: Messkriterien

Um dann in der Praxis einach kommunizieren zu können, schlagen wir ein Rating vor:

Rating	Interpretation	Recommendation
5	**Excellent Auditability** No impediments for audit.	System can be published for review.
4	**Good Auditability** Only small impediments for audit.	System can be published for review.
3	**Neutral Level of Auditability** Some moderate impediments for audit.	Publishing can be considered.
2	**Dubious Auditability** Several impediments for doing an audit.	Publishing not recommended.
1	**Bad Auditability** Serious impediments for doing an audit.	Not publishable.
n/a	**Not applicable**	Not applicable.

Abbildung 3: Rating

z. B. Namen von Privatpersonen, Passwörter usw.? Es muss auch sichergestellt werden, dass Lizenzen und IP-Rechte beachtet werden. Die Vollständigkeit des Codes ist ein weiterer wichtiger Aspekt, da oft der gesamte Code einer Anwendung überprüft werden muss.

Assessment und Rating

Um eine Software mit diesem Modell zu messen, werden die drei Aspekte in Messkriterien heruntergebrochen. Wir haben den Anspruch, dass jedes Messkriterium automatisch aus dem Code berechnet werden kann mit gängigen Analysesystemen, die in den Entwicklungsumgebungen mitgeliefert werden. Dadurch kann die Auditierbarkeit objektiv festgestellt werden.

Anwendung in der Praxis

Vorläufig identifizieren wir zwei Anwendungsfälle für das Modell der Auditierbarkeit:

1. Verifizierung von Software auf korrekte Funktionalität oder Einhaltung von Vorschriften.
2. Veröffentlichung von Software im Sinne der Vertrauensbildung.

In beiden Fällen sind die Eigentümer der Software (z. B. Behörden) dafür verantwortlich, dass ihre Software von Dritten leicht überprüft werden kann. Anwendungsgebiete sind kritische Infrastrukturen, in denen eine Fehlfunktion grosse Folgeschäden verursacht. In der Medizintechnik zum Beispiel bei der Steuerung von Bestrahlungsgeräten, im militärischen Bereich beim Einsatz von automatisierten Waffensystemen, aber auch z. B. Software, die zur Steuerung von Flugzeugen eingesetzt wird.

Der andere Bereich betrifft Software, die besonders sensible Daten verarbeitet oder Prozesse abbildet, die einer hohen Vertraulichkeit unterliegen. Dies ist z. B. Software für die elektronische Patientenakte (E-Health) oder das elektronische Wahlsystem.

Die Post hat deshalb den Quellcode ihres überarbeiteten E-Voting-Systems freigegeben. Der Code genügt den hier formulierten Anforderungen an die Auditierbarkeit.

Fazit

Software dringt zunehmend in kritische Bereiche unseres persönlichen und öffentlichen Lebens ein. Aus diesem Grund wird die Frage der Auditierbarkeit eine immer wichtigere Rolle spielen. Wir sind der Meinung, dass die Überprüfung der Nachvollziehbarkeit ein integraler Bestandteil eines jeden Überprüfungsprozesses sein sollte. Wenn zu erwarten ist, dass eine Software während ihrer Lebensdauer auditiert wird, dann ist es ratsam, die Auditierbarkeit als Qualitätsmerkmal von Beginn des Entwicklungsprozesses an einzubeziehen. Geschieht dies erst im Nachhinein, sind oft umfangreiche Nacharbeiten und Korrekturen erforderlich, und die damit verbundenen Kosten können unerschwinglich sein. Software kann Vertrauen schaffen, wenn sie von Anfang an mit Blick auf eine gute Auditierbarkeit geschrieben wird. Dann ist sichergestellt, dass Dritte im Code nachvollziehen können, was die Software tut. Die korrekte Funktionsweise kann dann von Personen mit den entsprechenden Kenntnissen bestätigt werden, und im Extremfall muss man sich nicht auf einen einzelnen Entwickler oder eine einzelne Institution verlassen. ■

CNO Panel No. 21

Das CNO Panel No. 21 findet am 25. Oktober 2021 im Casino Bern statt. Mit Thomas Ramge, Marc K. Peter, Patrick Gobonya, Cornelia Diethelm, Judith Bellaiche sind wiederum top Persönlichkeiten auf der Bühne dabei. Das CNO Panel ist die Schweizer Plattform für das Top-Management mit Schwerpunkt-Referaten, Workshops und viel Raum für persönliches Networking. Teilnehmende können sich auf relevante Statements aus Wissenschaft, Politik und Praxis – sowie auf Kunst und Kulinarik freuen. Der CNO Academy Workshop zum Thema «Auditierbarkeit von Software» findet am 25. Oktober am Nachmittag statt. «it business» ist Medienpartner. www.cno-panel.ch