Norbert Pohlmann, Helmut Reimer

Software Qualität – heute und morgen

Scheinbar ist alles geregelt! Das IT-Recht vermittelt den Eindruck, als seien die Konsequenzen fast jeder Abweichung vom Sollverhalten bei IT-Anwendungen durch die Zuordnung von Verantwortlichkeiten und dadurch bedingte Haftbarkeiten zu beschreiben und zu regulieren. Es gibt dazu eine Fülle von ‚Dokumentationen‘ mit entsprechenden Belehrungen. Beispielhaft sei hier auf den ‚Leitfaden Informationssicherheit – IT-Grundschutz kompakt‘¹ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) verwiesen. Die Lebenswirklichkeit vermittelt demgegenüber ein anderes Bild. Trotz der persönlichen Verantwortung der Vorstände und Geschäftsführer von Unternehmen für Versäumnisse und mangelnde Risikoversorge, können IT-Sicherheitsvorfälle nicht verhindert werden und die materiellen und ideellen Schäden nehmen weiter zu. Die Ursachen dafür sind vielfältig: In erster Linie steht die steigende Komplexität der IT-Systeme durch (zu schnelle) Integration neuer Anwendungen oder Leistungen in eine IT-Infrastruktur, die über Jahre gewachsen ist und zahlreiche historisch bedingte Angriffspunkte bietet. Ein drastisches Beispiel dafür ist die Tatsache, dass aktuell die Bankautomaten ihre Dienste mit dem Betriebssystem Windows XP leisten.

Eine Folge der Komplexität ist, dass IT-Systeme zu häufig schlecht konfiguriert sind. So sieht die diesbezügliche Analyse im BSI-Leitfaden aus:

„Durch Fehler bei der Administration entstehen in der Praxis die mit Abstand meisten Sicherheitslücken – und nicht etwa durch Softwarefehler. Würden die in Standardsoftware vorhandenen Sicherheitsfunktionalitäten vollständig und richtig ausgenutzt, so wäre das Sicherheitsniveau in Unternehmen und Behörden weitaus höher. Die Komplexität von Standard-Büroanwendungen steigt von Jahr zu Jahr. Sicherheit ist für Administratoren nur eine unter vielen, teils konkurrierenden Anforderungen in der täglichen Arbeit. Sie sind de facto kaum noch in der Lage, falsche (unsichere) Parametereinstellungen vollständig zu vermeiden. Vielen Betroffenen ist dieses Dilemma bewusst – doch ohne ausreichende Unterstützung seitens ihrer Vorgesetzten ist eine Änderung unrealistisch.“

Das klingt nicht nach schnellen Verbesserungsmöglichkeiten!

In allen IT-Anwendungen stellt aber die Software einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in PCs, Notebooks, Smartphones, Wearables, in sehr großen Rechenzentren, aber auch immer mehr in Autos, in Industrieanla-

gen, im Haus, usw. Deshalb lohnt es sich nach den bestimmenden Einflussfaktoren auf die Softwarequalität zu fragen.

Ein grundsätzliches Problem für die Softwarequalität ist eine statistische Fehlerdichte². Selbst bei sorgfältig geprüftem Softwarecode muss man heute mit einem Fehler auf 3.000 Zeilen Code rechnen. Für ein gängiges Betriebssystem mit typischerweise etwa 10 Mio. Zeile Code ist also mit 3.000 systematischen Softwarefehlern zu rechnen. Die Fehlerdichte wird sich im Laufe der Zeit verringern, Angreifer haben aber immer die Chance über diese potentiellen Schwachstellen in Systeme einzudringen und Schaden anzurichten.

Welche Wege weisen beispielhaft in die Zukunft?

- Ein wichtiger Faktor ist zweifellos der ‚gesellschaftliche‘ Umgang mit Software-Schwachstellen. Zero-Day-Schwachstellen sind Schwachstellen, die von Personen oder Organisationen gefunden wurden und nicht (sofort) den Herstellern gemeldet werden. Deshalb fehlen zunächst Updates. Geheimdienste, Strafverfolgungsbehörden oder kriminelle Organisationen, nutzen diese Schwachstellen erfolgreich. Das nicht sofortige weitergeben von Zero-Day-Schwachstellen sollte im Sinn des Schutzes unserer Gesellschaft unter Strafe gestellt werden, damit schnell auf neue Risiken reagiert werden kann.
- Die Hersteller müssen direkt für die Qualität der selbstentwickelten Software verantwortlich gemacht werden. Dies wird die Hersteller motivieren, die eigene Qualität entsprechend der vorhandenen Möglichkeiten zu optimieren.
- Wenn eine Schwachstelle an den Hersteller gemeldet wurde ist die unverzügliche Information der Anwender strikt einzuhalten und ein schadenbegrenzendes Update bereit zu halten. Hier haben die Hersteller ein sehr großes Potenzial vertrauensfördernd zu handeln. Auch dieser Prozess sollte durch eine besondere Haftung der Hersteller nachhaltig motiviert werden.
- Wenn ein Update zur Verfügung steht, sollten die Software-Nutzer dieses so schnell wie möglich einspielen, wo möglich sollte der Prozess voll automatisch ablaufen. Das Management des Updateprozesses sollte dabei ebenfalls in der Verantwortung der Hersteller liegen, weil diese den ganzen Updateprozess am besten und sichersten steuern können.

¹ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=1

² <https://de.wikipedia.org/wiki/Fehlerquotient>