Oliver Linssen et al. (Hrsg.): Projektmanagement und Vorgehensmodelle,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 247

Was fehlt (bisher) um Apps sicher zu entwickeln? – Prozesse, Werkzeuge und Schulungen für sichere Apps by Design

Katharina Altemeier[1], Matthias Becker[2], Stefan Dziwok[2], Thorsten Koch[2],
Sven Merschjohann[2]

Abstract: Mobile Apps sind ein wichtiger Treiber der Digitalisierung. Sie müssen heutzutage möglichst überall verfügbar sein – auf Smartphones, Tablets oder Arbeitsplatz-Rechnern und mit verschiedensten Geräten und Cloud-Diensten kommunizieren können. Neben dem steigenden Funktionsumfang und der zunehmenden Vernetzung dieser Applikationen, steigt auch die Komplexität der Sicherheitsanforderungen für App-Entwickler*innen. Die EU-Datenschutzverordnung (DSGVO) und andere sicherheitsrelevante Vorgaben sehen vor, dass Apps die Daten schützen müssen, sofern sie personenbezogene oder unternehmenskritische Informationen verarbeiten. Doch die Integration von Sicherheit in den Entwicklungsprozess stellt für viele Unternehmen noch eine große Herausforderung dar. Vor diesem Hintergrund möchte das Forschungsprojekt AppSecure.nrw Unternehmen für das Thema der sicheren Softwareentwicklung sensibilisieren und Entwickler*innen Möglichkeiten aufzeigen, wie sie mithilfe von Security-Prozessen und -Werkzeugen möglichen Bedrohungen in allen Phasen der Softwareentwicklung ganzheitlich entgegenwirken. In diesem Beitrag stellen wir Herausforderungen, Ziele sowie geplante Maßnahmen des Projekts vor. Ferner berichten wir über den aktuellen Stand einer von uns derzeit durchgeführten Studie, um Herausforderungen und Bedarfe an eine sichere Softwareentwicklung zu ermitteln.

Keywords: Security by Design, sichere Softwareentwicklung, Studie

1 Einleitung

Aufgrund der zunehmenden Digitalisierung werden immer mehr unternehmensspezifische Applikationen (Apps) für Smartphones, Webbrowser und Desktop-PCs entwickelt – sei es durch das Unternehmen selbst oder durch externe Dienstleister. Solche Apps sind entweder für den Endkunden, z.B. um Gesundheits- oder Finanzdaten zu verwalten, oder aber unternehmensinterne Apps, die Services, wie beispielsweise die Überwachung und Steuerung der Produktion, ermöglichen. In beiden Fällen werden fast immer sensible personenbezogene und/oder unternehmenskritische Daten verarbeitet. Der Schutz dieser Daten ist somit kritisch und der Verlust oftmals ein großer Schaden. Eine von IBM finanzierte Studie [IBM17] aus dem Jahr 2017 schätzt, dass der Verlust eines einzelnen sensitiven Datums in Deutschland einen Schaden von 160 US-Dollar verursacht, u.a. aufgrund des

[1] Fraunhofer IEM, Produktentstehung, Zukunftsmeile 1, 33102 Paderborn,
vorname.nachname@iem.fraunhofer.de
[2] Fraunhofer IEM, Softwaretechnik und IT-Sicherheit, Zukunftsmeile 1, 33102 Paderborn,
vorname.nachname@iem.fraunhofer.de

verlorenen Image. Zusätzlich sieht die im Mai 2018 in Kraft getretene EU-Datenschutzgrundverordnung (DSGVO) [EU16] finanzielle Sanktionen gegen Unternehmen vor, die personenbezogene Daten nicht ausreichend gegen Missbrauch schützen.

Die sichere Softwareentwicklung solcher Apps nimmt somit eine immer wichtigere Rolle ein. Erste, nicht repräsentative Erhebungen zeigen, dass das hierfür notwendige Security-Wissen beim Unternehmenspersonal kaum vorhanden ist und Experten für sichere Softwareentwicklung erst noch ausgebildet werden müssen. Zudem scheint es an geeigneten Prozessen und kostengünstigen sowie nutzerfreundlichen Werkzeugen zu fehlen. Um eine sichere Softwareentwicklung zu gewährleisten, benötigen Unternehmen somit heutzutage sehr hohe Anfangsinvestitionen. Darüber hinaus stellen externe Einflüsse auf die Entwickler*innen wie z.B. Zeitdruck, mangelnde Schulungsangebote sowie die fehlende Sensibilisierung aller an der Softwareentwicklung beteiligten Personen (insbesondere der Auftraggeber und Projektleiter) weitere Hindernisse dar, sodass das Thema der sicheren Softwareentwicklung oftmals nur sehr spät oder gar nicht angegangen wird (vgl. Abb. 1).

Abb. 1: Herausforderungen Entwickler*innen bei der Umsetzung einer sichereren Softwareentwicklung

Abb. 2: Maßnahmen um Entwickler*innen bei der Umsetzung einer sichereren Softwareentwicklung zu unterstützen

In diesem Papier stellen wir unser Forschungsprojekt "AppSecure.nrw - Security by Design von Java-basierten Applikationen" vor, das Fraunhofer IEM gemeinsam mit den Anwendungspartnern adesso mobile solutions GmbH, AXA Konzern AG und Connext Communication GmbH bis Ende 2021 bearbeitet. In Abb. 2 sind die Ziele des Projekts dargestellt, welche die Entwickler*innen bei der Entwicklung sicherer Software unterstützen sollen. Dazu gehört zum einen die Sensibilisierung aller im Projekt Beteiligten bezüglich der Notwendigkeit von Security und gleichzeitig ein entsprechender Wissensaufbau durch verschiedene Schulungen. Darüber hinaus sollen existierende Methoden und Prozesse verbessert werden und so ein Secure Software Development Lifecycle (Secure-SDLC) definiert werden, der bedarfsgerecht auf die Bedürfnisse eines Unternehmens angewendet

werden kann. Innerhalb des Secure-SDLCs wird der Einsatz verschiedener kostenloser Werkzeuge vorgesehen, um Entwickler*innen durch die Automatisierung von Aufgaben zu entlasten. Somit sollen Anfangsinvestitionen reduziert sowie das Risiko vor finanziellen Schäden (z.B. aufgrund von Imageschäden oder Sanktionen) gesenkt werden. Die Kernidee ist, dass der Sicherheitsaspekt von Anfang an in der Entwicklung berücksichtigt wird. Letztlich soll ein Security by Design-Instrumentarium entstehen, welches nicht nur die notwendigen Prozesse, sondern auch die dazugehörigen Werkzeuge und Entwicklerrollen inkl. ihrer Qualifikation umfasst.

In diesem Beitrag stellen wir Herausforderungen, Ziele, Aufbau und geplante Maßnahmen des Projekts vor und berichten über den aktuellen Stand unserer Studie, deren Ergebnisse ab Ende September verfügbar sein sollten. Im nachfolgenden Kapitel 2 gehen wir zunächst auf den Aufbau des Projekts ein, bevor wir die einzelnen Maßnahmen näher vorstellen. Kapitel 3 schließt mit der Zusammenfassung des Papiers.

2 Aufbau des Projekts

Das Projekt hat Anfang 2019 begonnen und wird über eine dreijährige Laufzeit bis Ende 2021 vom Fraunhofer IEM und den drei Anwendungspartnern, adesso mobile solutions GmbH, AXA Konzern AG und Connext Communication GmbH bearbeitet. Die Rolle der Anwendungspartner ist dabei, Informationen zu dem aktuellen Entwicklungsstand beizutragen, sowie die entwickelten Methoden und Werkzeuge während des Projekts zu erproben und Feedback zurückzuspielen. Dadurch wird sichergestellt, dass die Ergebnisse des Forschungsprojekts die realen Bedarfe der Industrie berücksichtigen und eine hohe Qualität aufweisen. So wird es den Unternehmen ermöglicht, diese schon während des Projekts in der Praxis einzusetzen.

In Abb. 3 ist der grobe Zeitplan des Projekts zu sehen. Vorbereitend wird mittels unserer Studie «Secure Software Engineering in Unternehmen der DACH-Region» der Stand der sicheren Softwareentwicklung in Unternehmen der DACH-Region (Deutschland, Österreich, Schweiz) evaluiert. Diese Informationen helfen uns, darauf basierend ein bedarfsgerechtes Instrumentarium aufzusetzen und entsprechend benötigte Schulungen zu konzipieren und durchzuführen. Der wesentliche Fokus des Projekts liegt dabei auf der bedarfsgerechten Anpassung und Weiterentwicklung von Codeanalyse-Werkzeugen für Java durch permanentes Feedback der Anwendungspartner. Im Folgenden werden die einzelnen Maßnahmen detailliert beschrieben.

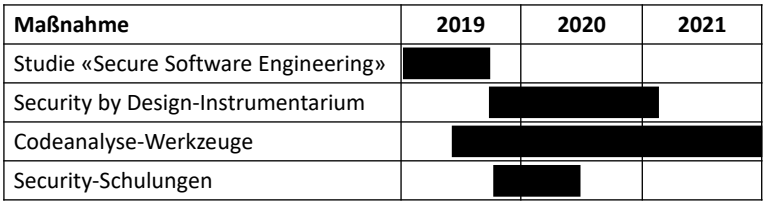

Abb. 3: Zeitplan des Projekts

2.1 Studie «Secure Software Engineering in Unternehmen der DACH-Region»

Ein wesentliches Ziel unseres Forschungsprojekts ist es, das Security by Design-Instrumentarium eng auf die aktuellen Kenntnisse und Bedarfe der Entwickler*innen abzustimmen. Um dieses Ziel zu erreichen, haben wir vorbereitend damit begonnen, die Studie «Secure Software Engineering in Unternehmen der DACH-Region» zu konzipieren und durchzuführen. Diese besteht aus insgesamt drei Teilen.

Im ersten Teil der Studie werden Entwickler*innen aus der gesamten DACH-Region mit Hilfe eines Online-Fragebogens befragt, um dadurch einen umfassenden Kenntnisstand der Entwickler*innen bezüglich Security zu erheben.

Im zweiten Teil der Studie werden ausgewiesene Experten der drei Anwendungspartner interviewt, um so deren derzeitigen Kenntnisstand einschätzen zu können, sowie bereits im Einsatz befindliche Security-Prozesse und -Werkzeuge zu ermitteln. Die Interviews werden durchgeführt, sobald eine hohe Anzahl an Fragebögen ausgefüllt und vorläufig ausgewertet worden ist. So helfen die Interviews bei der Interpretation und beim Verständnis auffälliger Aussagen innerhalb der Online-Fragebögen.

Im dritten und unternehmensspezifischen Teil der Studie werden bereitgestellte App- und Webanwendungen stichprobenartig mit verfügbaren Security-Werkzeugen analysiert, um ggf. unternehmensspezifische Security-Themen für Schulungen zu identifizieren.

2.2 Security by Design-Instrumentarium für die App- und Webentwicklung

Aufbauend auf den Ergebnissen der Studie, werden wir einen allgemeinen Secure by Design Development Lifecycle für die sichere Entwicklung von App- und Webanwendungen definieren. Der entstehende Referenzprozess lehnt sich an den allgemeinen Softwareentwicklungsprozessen an und wird durch Maßnahmen und Werkzeuge nach dem aktuellen Stand der Technik zu einem Security by Design-Instrumentarium ergänzt.

Zusätzlich soll der Referenzprozess die Bedarfe der drei Anwendungspartner berücksichtigen. Aufgrund ihrer Diversität bezüglich des Security-Kenntnisstands der Mitarbeiter, genutzter Werkzeuge, Entwicklungsprozesse, Branchen sowie Firmengröße werden drei deutlich unterschiedliche Ausprägungen eines Secure-SDLCs erwartet. Nach Aufnahme der unternehmensspezifischen Prozesse werden Gemeinsamkeiten und Unterschiede herausgearbeitet und gemeinsam diskutiert. Die gewonnenen Erkenntnisse dienen als weitere Grundlage für die Definition des unternehmensunabhängigen und anpassbaren Referenzprozesses.

2.3 Bedarfsgerechte und benutzerfreundliche Codeanalyse-Werkzeuge

Ein wesentliches Merkmal des zu entwickelnden Secure-SDLCs soll die bedarfsgerechte Integration verschiedener Werkzeuge zur Sicherstellung der Security sein. Im Anwendungsbereich der statischen Codeanalyse existieren verschiedene Open Source-Werkzeuge, die maßgeblich zur Verbesserung der Datensicherheit beitragen (z.B. FlowDroid [Ar14] und CogniCrypt [Kr17] [Ecl2019]) und sich damit sehr gut für die Integration in den zu entwickelnden Secure-SDLC eignen. Aktuell werden jedoch Security-Experten mit

solidem Vorwissen im Bereich Security benötigt, um diese sinnvoll anwenden zu können. Damit auch Entwickler*innen mit weniger Vorwissen diese Werkzeuge nutzenstiftend und effizient einsetzen können, werden die Open Source-Werkzeuge mit Hilfe ständigem Feedbacks der Anwendungspartner bedarfsgerecht und benutzerfreundlich angepasst und weiterentwickelt.

2.4 Security-Schulungen für die App- und Webentwicklung

Abschließend sollen basierend auf den verschiedenen Projektergebnissen Schulungsblöcke für Entwickler*innen bezüglich Security konzipiert und durchgeführt werden. Die Schulungen sollen theoretische Betrachtungen mit praktischen Erprobungen von Methoden und Werkzeugen vereinen. Damit bieten die Schulungsblöcke die Möglichkeit, Unternehmen bei der Einführung entsprechender Codeanalyse-Werkzeuge zu unterstützen und die Effizienz bei der Sicherstellung der Datensicherheit deutlich zu steigern.

3 Zusammenfassung

Die sichere Entwicklung von Applikationen für das Smartphone oder den Webbrowser stellt eine zunehmende Herausforderung für Entwickler*innen dar. Dies liegt zum einem an dem steigenden Funktionsumfang und zum anderen an den hohen Auflagen, die beim Schutz von personenbezogenen Daten erfüllt werden müssen. In diesem Beitrag haben wir die Herausforderungen, Ziele und geplanten Maßnahmen unseres Forschungsprojekts AppSecure.nrw vorgestellt. Innerhalb des Projekts wollen wir Entwickler*innen ganzheitlich bei der Umsetzung einer sicheren Softwareentwicklung unterstützen. Daher wird in enger Zusammenarbeit mit den Anwendungspartnern ein Security by Design-Instrumentarium entwickelt, dass neben anpassbaren Prozessen und kostenlosen Werkzeugen, auch ein abgestimmtes Schulungsangebot enthält. Das Instrumentarium wird auf die Bedarfe der Anwendungspartner angepasst und in ihre Prozesse integriert. Basierend auf dem Feedback der Anwendungspartner, werden die Prozesse, Werkzeuge und konzipierten Schulungen fortwährend verbessert. Bereits Ende September werden erste Ergebnisse unserer Studie zur sicheren Softwareentwicklung im deutschsprachigen Raum erwartet.

Danksagung

Diese Arbeit ist Teil des Forschungsvorhabens „AppSecure.nrw – Security-by-Design von Java-basierten Applikationen“. Das Vorhaben wird aus Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE) gefördert.

Literaturverzeichnis

[Ar14] Arzt, S.; Rasthofer, S.; Fritz, C; Bodden, E.; Bartel, A.; Klein, J; Le Traon, Y.; Octeau, D.; McDaniel, P. D.: FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps., PLDI. 2014.

[Ecl2019] Eclipse CogniCrypt. https://projects.eclipse.org/proposals/eclipsecognicrypt

[EU16] Europäische Union (EU): Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). (*ABl. (Amtsblatt der Europäischen Union)* (L 119/1)).

[IBM17] IBM Security: Cost of Data Breach Study, 2017.

[Kr17] Krüger, S.; Nadi, S.; Reif, M.; Ali, K.; Mezini, M.; Bodden, E.: CogniCrypt: Supporting Developers in using Cryptography. ASE 2017, Tool Demo.