HITSSSE
Höhere IT-Sicherheit durch
Sichere Software Entwicklung

IT-Sicherheit
IN DER WIRTSCHAFT

Secure Coding mit Security User Stories

Eine Einführung mit Beispielen

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Disclaimer

Dieses Dokument wurde im Oktober 2022 erstellt. Jegliche Erklärungen, Einschätzungen und betrachteten Methoden sind unabhängig von Dritten erstellt worden und deshalb „anbieterneutral“. Jegliche hier dargestellten Informationen werden ohne Gewähr zur Verfügung gestellt. Sie dienen als Hilfestellung und sollten erst nach eigener Evaluation verwendet werden.

1 Motivation

In agilen Softwareentwicklungs-Prozessen steht der Nutzer im Mittelpunkt. Der Fokus gilt dem Mehrwert für Endbenutzer und Stakeholder. Damit verlagert sich der Schwerpunkt weg vom reinen Entwurf und der Programmierung von Software. User Stories sind eine essentielle Komponente dieses Konzeptes. Das aktuell in der Praxis am meisten genutzte agile Konzept ist Scrum.

Das Thema Sicherheit ist so früh wie möglich im Prozess der Softwareentwicklung zu berücksichtigen. Dafür eignet sich der Zeitpunkt der Erstellung von User Stories - denn diese werden zu Beginn eines agilen Entwicklungsprozesses erstellt. Diese Dokument gibt daher eine Einführung zum Einsatz von speziellen *Security User Stories*. Zum besseren Verständnis werden die grundsätzlichen Prinzipien von agilen Methoden kurz aufgegriffen. Beispiele erläutern die Anwendung in der Praxis. Die folgenden Fragen führen durch das Dokument:

Was sind agile Methoden und welche Vorteile bieten sie in der Softwareentwicklung?
Was ist eine (Security) User Story?
Was sind die Vorteile einer Security User Story?
Wie schreibe ich eine Security User Story?

Ziel des Dokuments ist es, einen Überblick zum Einsatz von Security User Stories in der Softwareentwicklung zu vermitteln. Darüber hinaus bietet das Dokument Beispiele und weiterführende Litaratur zur Vertiefung in der Praxis an. Am Ende des Dokuments soll eine bessere Abschätzung getroffen werden können, welchen Nutzen Security User Stories in der Softwareentwicklung bieten und der Einsatz im eigenen Unternehmen in Frage kommt.

2 Agile Methoden und deren Vorteile in der Softwareentwicklung

In dem nachfolgenden Abschnitt wird kurz auf das grundlegende Konzept von agilen Methoden eigegangen und der Nutzen innerhalb der Softwareentwicklung aufgezeigt.

2.1 Agiles Manifest

Unter agilen Konzepten ist eine Sammlung von Methoden und Vorgehensweisen zu verstehen. Diese sind daraufhin optimiert, bei den spezifischen Problemen zu helfen, denen sich Softwareteams gegenübersehen. Zusätzlich sind sie so einfach gehalten, dass sie sich möglichst einfach umsetzen lassen. Diese Methoden und Vorgehensweisen betreffen alle Bereiche der klassischen Softwareentwicklung. Dazu zählen Projektmanagement, Softwaredesign und -architektur sowie Prozessoptimierungen. Alle Methoden und Vorgehensweisen bestehen aus

Abbildung 1: Werte des agilen Manifestes

Praktiken, die vereinfacht und optimiert wurden, um sie so leicht wie möglich umsetzen zu können. [1]

In den USA wurde in den 90er Jahren eine Ära der schlanken Softwareentwicklung angestoßen, daraus ist das in Abbildung 1 dargestellte agile Manifest entstanden. Es umfasst vier grundlegende Werte [2]. An dieser Stelle ist wichtig zu verdeutlichen: Obwohl die Werte auf der rechten Seite wichtig sind, sind die Werte auf der linken Seite höher zu priorisieren.

Bereits Fred Brooks, ein Pioneer im Bereich der Softwareentwicklung, hatte in den 1980er Jahren in seinem Artikel *No Sivler Bullet: Essence and Accidents of Software Engineering* [3] die Erkenntnis, dass keine einheitliche Lösung für das Erstellen von Software existiert. Brooks' Einschätzung wird auch heute noch geteilt [4]. Agile Methoden sind keine festen Vorgaben. Vielmehr handelt es sich um eine Sammlung aus Methoden, Konzepten und Vorgehensweisen, die einen Rahmen für Software-Teams bieten, innerhalb dessen sie sich frei bewegen können.

2.2 Vorteile agiler Methoden

Agile Methoden bieten verschiedene Vorteile. Einige davon sind in Abbildung 2 aufgelistet.

Hierbei muss allerdings hervorgehoben werden, dass die Vorteile agiler Methoden nur ausgeschöpft werden können, wenn die Methoden auf das Entwicklerteam und die Projektanforderungen angepasst werden. Es sollte daher stets darauf geachtet werden, dass der agile Gedanke aktiv gelebt wird und nicht zur reinen Zweckerfüllung reduziert wird.

3 (Security) User Stories

Aufbauend auf der Grundlage von User Stories werden im Nachfolgenden Security User Stories vorgestellt.

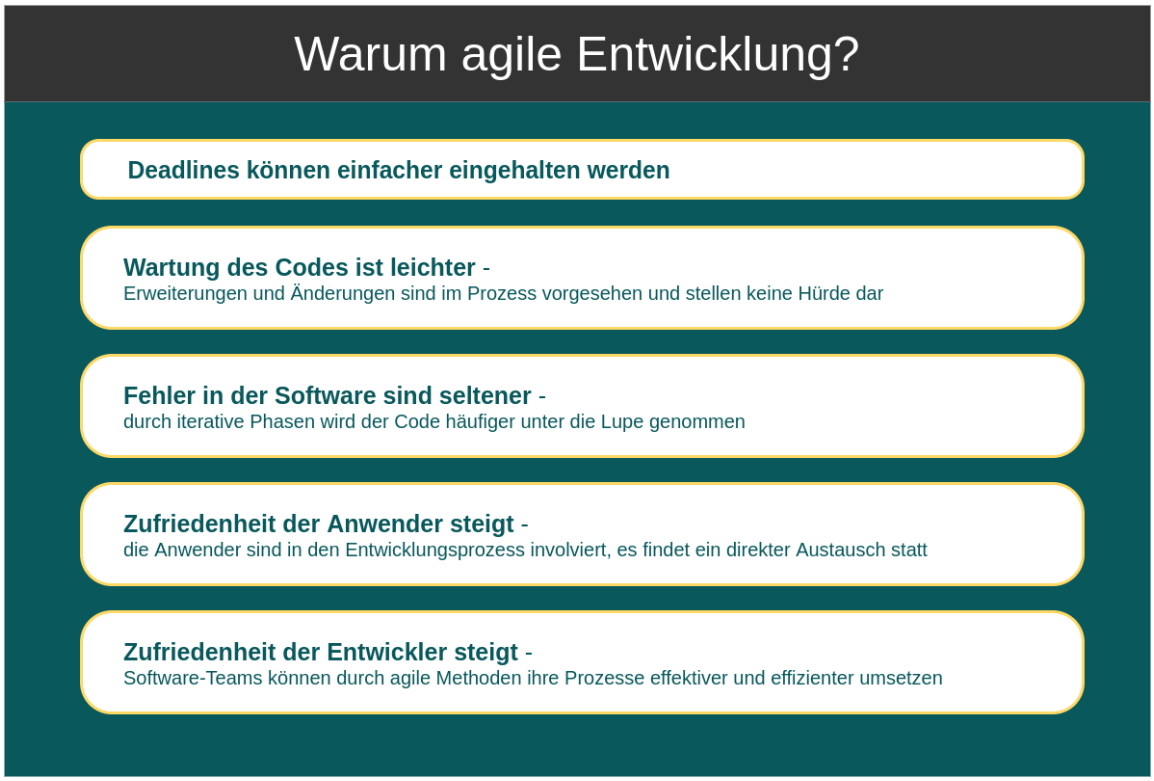
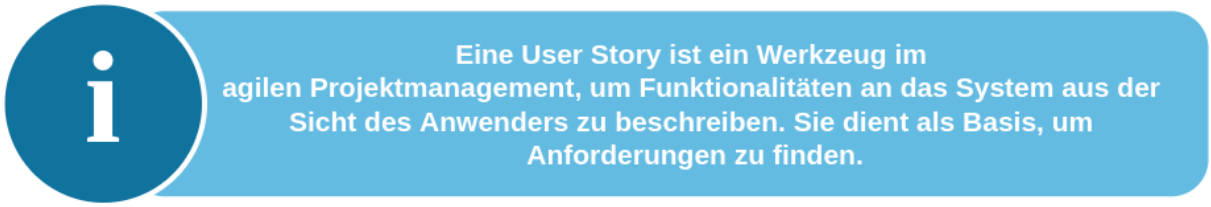


Abbildung 2: Vorteile der agilen Softwareentwicklung - ein Auszug.

3.1 Was ist eine (Security) User Story?

Um zu verstehen, was Anwender einer Software konkret brauchen, helfen sogenannte User Stories - sie lassen Software-Teams besser verstehen, welcher Bedarf bei den Anwendern besteht. Eine User Story ist eine sehr kurze Beschreibung einer konkreten Sache, die der Kunde in seiner Anwendung braucht. Häufig wird es auch als ein Werkzeug verstanden, um Funktionalitäten an das System aus der Sicht des Anwenders zu beschreiben. Diese Basis dient dazu, um Anforderungen an die zukünftige Software zu definieren. Eine Security User Story ist eine Spezialisierung einer User Story. Security User Stories beschreiben den konkreten Bedarf zu Themen der Sicherheit innerhalb der Softwareentwicklung.



3.2 Was sind die Vorteile einer Security User Story?

Das Thema IT-Sicherheit soll fest im Prozess der Softwareentwicklung verankert sein – und das möglichst zum Start des Entwicklungszyklus, d.h. bereits bei den Gesprächen mit den Kunden muss die Sicherheit mit berücksichtigt werden. Die Spezialisierung der klassischen User Story

zu einer Security User Story ermöglicht es, das Thema IT-Sicherheit so früh wie möglich im Entwicklungsprozess zu integrieren. Daraus ergeben sich die folgenden konkreten Vorteile:

- Security-Themen von Anfang an in den Entwicklungsprozess einbeziehen
- Mehr Zeit, um Sicherheitslücken zu schließen
- Security-Themen sind gleich gewichtet, wie andere Stories
- Security-Themen werden immer wieder in Erinnerung gerufen
- Security-Themen werden messbar (X Security Stories sind abgeschlossen)

3.3 Wie schreibe ich eine Security User Story?

Für das Verfassen von Security User Stories ist es hilfreich, das allgemein in der Praxis eingesetzte Grundgerüst zu verwenden: **Als <Kundentyp> möchte ich ..., um...(Nutzen) zu erreichen.**

Die folgende Check-Liste unterstützt beim Erstellen einer Security User Story:

- So klein wie möglich halten: Die Story soll innerhalb einer Entwicklungsiteration umsetzbar sein.
- So einfach wie möglich halten: Die Story soll aus Sicht des Nutzers erstellt sein und keine technischen Details enthalten.
- Der Mehrwert muss klar erkennbar sein, d.h. der Nutzen der Story
- Es soll eine Sache beschrieben sein. Ist es erforderlich, muss die Story in mehrere Stories aufgeteilt werden. Man spricht hier vom sogenannten Splitting.
- Stories sollten im Team geschrieben werden
- Einsatz von Akzeptanzkriterien zur Prüfung der Mindestanforderungen

Akzeptanzkriterien: Mit Hilfe von Security User Stories können sich Teams einerseits auf die Bedürfnisse, Wünsche und Werte ihrer Kunden konzentrieren und andererseits auf die Aktivitäten, die sie durchführen müssen, um diese Werte zu schaffen. Das Bindeglied, das diese beiden Dinge miteinander verbindet, sind die sogenannten Akzeptanzkriterien. Akzeptanzkriterien liefern einen detaillierten Blick auf die Anforderungen eines Benutzers. Sie helfen dem Team, die Bedingungen zu definieren, nach dem eine Security User Story als abgeschlossen gilt.

3.4 Wie kann ich die Qualität einer Security User Story verbessern?

Ein allgemein anerkanntes Prinzip, nachdem man die Qualität einer Security User Story bewerten und verbessern kann, ist das sogenannte **INVEST Prinzip**:

- **Independent/Unabhängig:** Die Story kann für sich stehen, ohne von anderen Storys abhängig zu sein.
- **Negotiable/Verhandelbar:** Die Story umfasst am Anfang wenige Details und wird nach und nach in Diskussion detaillierter.
- **Valuable/Wertvoll:** Die Story bringt Anwender/Kunden einen Mehrwert.
- **Estimable/Schätzbar:** Der Aufwand der Story lässt sich durch Entwickler schätzen.

- **Small/Klein:** Die Story muss innerhalb einer Iteration implementierbar sein.
- **Testable/Testbar:** Die Story muss sich überprüfen lassen können.

In Abbildung 3 sind die wichtigsten Punkte zum Erstellen einer Security User Story zusammengefasst.

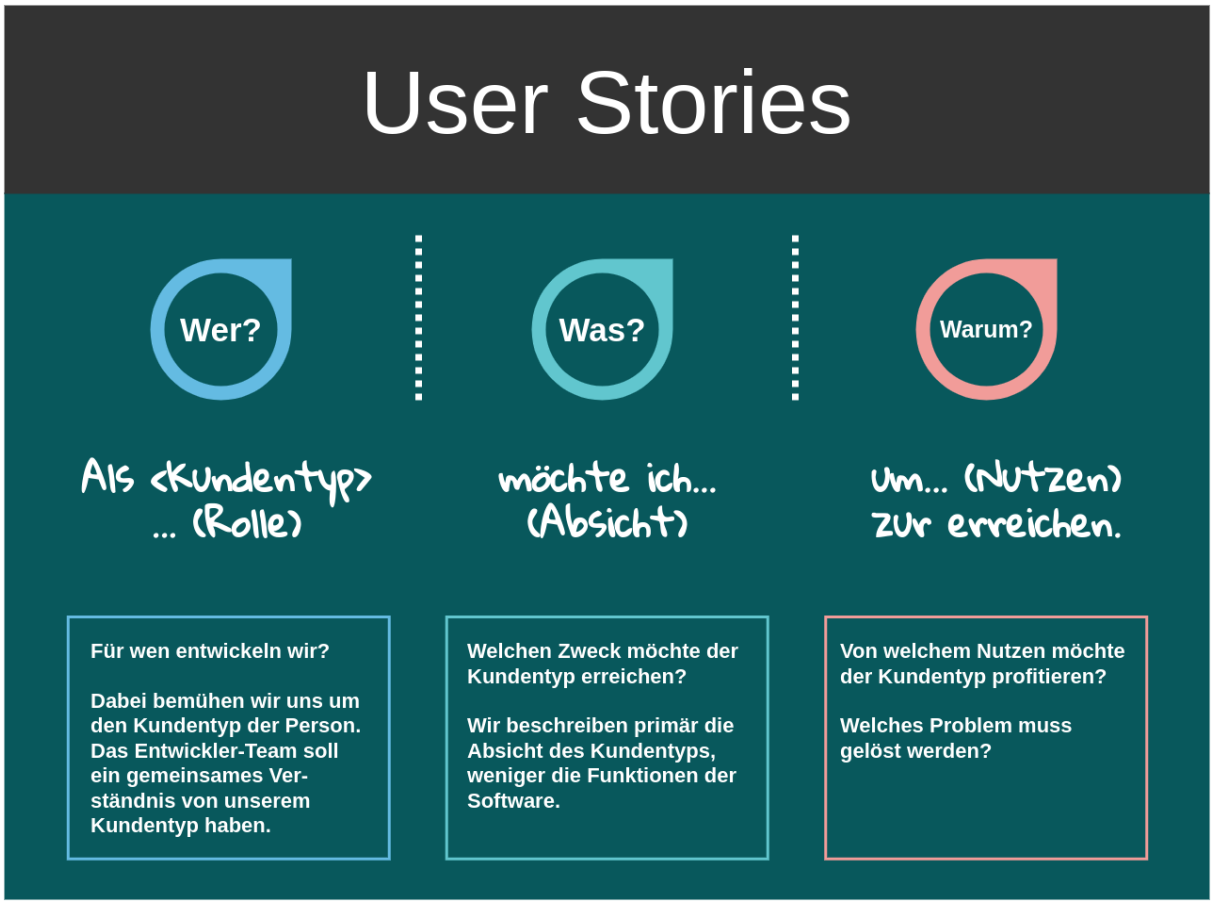


Abbildung 3: Zusammenfassung zur Erstellung einer Security User Story

4 Security User Stories - Beispiele und Anwendung

Das *Open Web Application Security Project* [5] bietet eine Übersicht zu Beispielen für Security User Stories. In Anlehnung an diese Arbeit enthält Tabelle 1 einen Auszug an Beispielen.

Tabelle 1: **Security User Stories - Beispiele**

Security User Story	Akzeptanzkriterium
Als Betreiber eines Datencenters muss ich alle Verbindungen zu einer Anwendung authentifizieren, um die Benutzerdaten zu schützen.	Es ist sichergestellt, dass alle Verbindungen zu Anwendungen, die Kundeninformationen oder -funktionen enthalten, authentifiziert sind.
Als Kunde eines Softwareunternehmens möchte ich bei der Eingabe von Passwörtern und anderen Feldern das Zwischenspeichern oder automatische Ausfüllen unterbinden, weil sie sensiblen Informationen enthalten.	Es muss sichergestellt sein, dass Passwörter und andere Dateneingabefelder, die sensible Informationen enthalten, nicht zwischengespeichert werden und keine automatische Vervollständigung zulassen. Für Passwort-Manager kann eine Ausnahme gemacht werden.
Als Nutzer Max Hoffmann möchte ich, dass die Anwendung alle Eingaben überprüft, um ihre Korrektheit und Eignung für den vorgesehenen Zweck zu garantieren.	Alle Daten, die von einem externen Unternehmen oder Kunden eingegeben werden, müssen validiert werden.
Als Anlagenbetreiber benötige ich einen sicher verwalteten Zugang zu den Produktionsanlagen, um die dort gespeicherten geheimen Schlüssel zu schützen.	Es gibt eine explizite Richtlinie dafür, wie kryptografische Schlüssel verwaltet werden (z. B. Erzeugung, Verteilung, Widerruf und Ablauf).
Als Administrator einer Datenbank möchte ich, dass die Anwendung unbefugte Versuche, auf meine Daten zuzugreifen, sich anzumelden oder Änderungen vorzunehmen, erkennt und meldet, um Sicherheitsvorfälle überwachen zu können.	Es besteht die Möglichkeit, die Anzahl der Anmeldeversuche zu begrenzen oder Warnungen zu senden, wenn Schwellenwerte überschritten wurden. Zusätzlich gibt es Warnungen, wenn eine Rolle eine Aktion versucht, die über die Berechtigungsstufe hinausgeht, oder wenn die Versuche, die Berechtigungsstufe zu überschreiten, einen Schwellenwert erreichen.

5 Zusammenfassung

Agil Arbeiten und dabei den Ansprüchen an IT-Sicherheit zu genügen, fällt vielen Entwickler-Teams schwer. Daher ist es wichtig, IT-Sicherheit als festen Bestandteil des Entwicklungs-Prozesses zu etablieren und so im eigenen Rhythmus kontinuierlich die Sicherheit zu verbessern. Security User Stories sind ein geeignetes Mittel, um das Thema Sicherheit so früh wie möglich im Entwicklungsprozess von Software zu berücksichtigen und Entwickler-Teams dabei zu unterstützen die Sicherheit von Software zu erhöhen.

Literatur

[1] A. Stellman, J. Greene, and T. Demmig, *Agile Methoden von Kopf bis Fuß*. Von Kopf bis Fuß, O'Reilly, 2018.

[2] N. Weiß, *Agile Business Intelligence. Begriffe, Methoden, Analysen*. Recht, Wirtschaft, Steuern, Igel Verlag RWS, 2018.

[3] F. P. Brooks, “No silver bullet: Essence and accidents of software engineering,” *IEEE computer*, vol. 20, no. 4, pp. 10–19, 1987.

[4] D. A. Grier, “There is still no silver bullet,” *Computer*, vol. 54, no. 2, pp. 60–62, 2021.

[5] O. W. A. S. P. (OWASP)", “Collection of user security stories,” *https://github.com/OWASP/user-security-stories*, 2018.

Impressum und Kontakt

Projekt HITSSSE – Höhere IT-Sicherheit durch Sichere Software Entwicklung

Immer mehr kleine und mittlere Unternehmen (KMUs) entwickeln Software für eigene Infrastrukturen oder Produkte. Hierbei herrscht meist ein hoher Zeitdruck und es stehen oft nur beschränkt personelle Ressourcen zur Verfügung. Oft werden inzwischen auch agile Softwareentwicklungsmethoden eingesetzt, die schnell einsetzbare Lösungen liefern sollen. Dadurch spielt die Sicherheit dieser Software oft eine untergeordnete Rolle, was sich letztendlich auch auf die IT-Sicherheit dieser Unternehmen und ihrer Kunden auswirkt. Im Fördervorhaben HITSSSE soll die IT-Sicherheit durch sichere Software Entwicklung für KMUs verbessert werden. Hierfür werden im Forschungsprojekt Handlungsempfehlungen sowie technische Hilfsmittel erstellt, die zuerst bei den assoziierten Partnern des Projekts konkret erprobt werden, um daraufhin generische Lösungsansätze für kleine und mittlere Unternehmen in Deutschland zu schaffen. Durch die Zusammenarbeit mit der Transferstelle „IT-Sicherheit in der Wirtschaft" soll die Breitenwirkung der entwickelten Angebote verstärkt werden. Gefördert wird das Projekt HITSSSE durch das Bundesministerium für Wirtschaft und Klimaschutz im Förderschwerpunkt Mittelstand-Digital. www.hitssse.de

Projektleitung

Prof. Dr.-Ing. Dominik Merli
Leiter HSA_innos
dominik.merli@hs-augsburg.de

Prof. Dr.-Ing. Alexandra Teynor
Leiterin HSA_ias
alexandra.teynor@hs-augsburg.de

Prof. Dr. Phillip Heidegger
HSA_ias
phillip.heidegger@hs-augsburg.de

Autor

Susanne Kießling, M.Sc.

HSA_innos – Institut für innovative Sicherheit

HSA_innos hilft Unternehmen dabei, sich individuell zu schützen. Neben der Aus- und Weiterbildung von Sicherheitsexperten liegt der Schwerpunkt des Instituts auf der Entwicklung von Technologien und Prozessen für die IT-Sicherheit zur Anwendung in der Praxis. Zusammen mit HSA_innos schützen Unternehmen und andere Organisationen ihre Investitionen und Kunden vor digitalen Bedrohungen. Mehr Informationen zu HSA_innos finden Sie unter www.hsainnos.de.

HSA_innos
Institut für innovative Sicherheit

Hochschule **Augsburg** University of Applied Sciences

HSA_ias – Institut für agile Softwareentwicklung

Das Institut für agile Softwareentwicklung (HSA_ias) forscht in enger Zusammenarbeit mit Partnern aus Industrie und Wissenschaft zu den Schwerpunkten agile Softwareentwicklung, Programmiersprachen & Sicherheit, Prozessdigitalisierung sowie Anwendungen der KI. Die hierbei entstehenden Projekte decken eine breites Feld an Anwendungen ab, wie z.B. digitale Gesundheit, Produktionstechnik oder Digitalisierung der öffentlichen Verwaltung. Die Aus- und Weiterbildung von Software-IngenieurInnen für die Herausforderungen der Zukunft ist dabei ein zentrales Anliegen des Instituts.

Mittelstand Digital

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der *Initiative IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Mittelstand-Digital