Sicherheitsanforderungen: oft vernachlässigt, dabei sehr nützlich!

Prof. Dr. Sachar Paulus
Fachhochschule Brandenburg

OWASP
The Open Web Application Security Project

Elevator Pitch

OWASP
The Open Web Application Security Project

- Sicherheitsanforderungen machen es deutlich leichter, sichere Software zu bauen
- Sicherheitsanforderungen sind in der Verantwortung des Kunden
- Wichtig: explizite Anforderungen beschreiben
- Mit testbaren Akzeptanzkriterien
- Lebendes Dokument!

About Me

OWASP
The Open Web Application Security Project

- Professor für Wirtschaftsinformatik und Security Management
- Vorstandsvorsitzender von ISSECO (CPSSE Zertifizierung)
- 8 Jahre SAP, davon 4 Jahre verantwortlich für Produktsicherheit

Fachhochschule Brandenburg
University of Applied Sciences

ISSECO®
SECURE SOFTWARE ENGINEERING

Was sind Sicherheitsanforderungen?

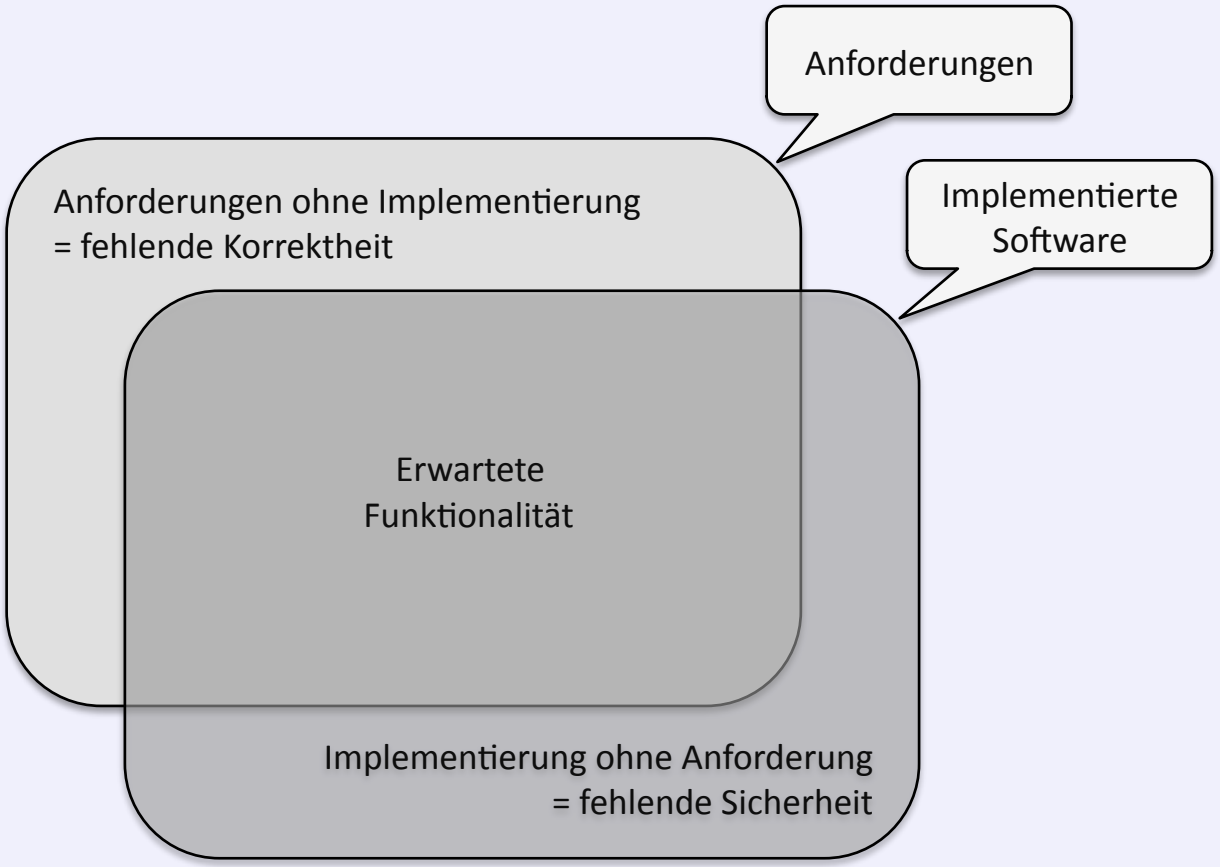
OWASP
The Open Web Application Security Project

- Anforderungen = Erfüllung von Use Cases
  - Funktionale Anforderungen
  - Nicht-funktionale Anforderungen

    (= Mis-Use Cases)

- Sicherheitsanforderungen sind - in der Regel - nicht-funktional!!

OWASP
The Open Web Application Security Project



Status Quo

OWASP
The Open Web Application Security Project

- Kunden kennen ihre Sicherheitsanforderungen nicht
- Kunden verlagern die Verantwortung der Ermittlung der Sicherheitsanforderungen an den Dienstleister
  - Grund: „Sicherheit ist immer gleich“
- Dienstleister nehmen Kataloge und achten auf Dinge, die sie kennen
- ==> keine adäquate Sicherheit, evtl. trotzdem hohe Kosten!

Ziel

OWASP
The Open Web Application Security Project

- Kunden müssen in die Lage versetzt werden, ihre Sicherheitsanforderungen zu kennen
  - Workshop
    - mit der Fachabteilung!
  - (High-level) threat modeling
  - *Branchenspezifische* Kataloge
  - *Anwendungsspezifische* Best Practices

Beispiel

OWASP
The Open Web Application Security Project

Nr	(Mis-) Use Case	F / NF	Akzeptanztest	Sicherheits-maßnahme	Priorität	Verant.-wortlich
1	Als Student kann ich persönliche Vorlesungen ergänzen und zwar über eine serverseitige Konfiguration (z.B. mittels Checkbox)	F	Klicke fünf Checkboxen an und übernehme diesen in den Kalender. Im Anschluss prüfe ob diese in dem caldav kompatiblen Kalender-Produkt übernommen wurden.		...	...
2	Als User muss ich mich authentifizieren, um Veränderungen vornehmen zu können.	NF	Versuche ohne Authentifizierung zehn mal veränderungen vorzunehmen. Stelle fest, dass diese nicht übernommen wurden.	Verwendung von LDAP Auth	...	...
3	Als User muss ich mich authentifizieren, um an personalisierte Inhalte zu gelangen.	NF	Versuchen ohne Authentifizierung zehn mal an personalisierten Inhalte zu gelangen. Stelle fest, dass dies nicht funktioniert.	Verwendung von LDAP Auth	...	...
4	Als User kann ich meine FH-Zugangsdaten für den Login verwenden.	F	Verwende deine FH-Zugangsdaten um dich einzuloggen und stelle fest,dass du eingeloggt bist.	Verwendung von LDAP Auth	...	...
5	Als User kann ich persönliche Termine aus meinem Kalender entfernen. (z.B. mittels Checkbox)	F	Wähle fünf Checkboxen ab und prüfe, ob diese in deinem caldav kompatiblen Kalender-Produkt übernommen wurden.		...	...
6	Als User kann ich in der Webanwendung meinen Studiengang und mein Semester einpflegen.	F	Trage als User dein Semester und Studiengang in dein persönliches Profil ein und überprüfe auf Erfolg.		...	...
7	Ein Hacker kann keine Informationen verändern, während ich sie einstelle.	NF	Versuche eine aktuell genutzte Verbindung mit einem geeigneten Tool innerhalb von 10 Minuten abzuhören, und stelle fest, dass dies nicht funktioniert.	Verwendung von TLS	...	...

Wichtig!

OWASP
The Open Web Application Security Project

- Anforderungskatalog auch für die Definition von Test Cases nutzen
- Akzeptanzkriterien definieren
  - gerade bei nicht-funktionalen Anwendungen
  - Bewusste Entscheidung!
- Dokument nachhalten („living document“)

Akzeptanzkriterien

OWASP
The Open Web Application Security Project

- Nicht-funktionale Sicherheitsanforderungen erfordern i.d.R. die Abwesenheit von Möglichkeiten
  - 100% Nachweis nicht möglich
- Erforderlich: bewusste Entscheidung für „ab da ok“
- In der Praxis: Fuzzing, Anzahl der Durchläufe, der Vektoren,...

Fazit

OWASP
The Open Web Application Security Project

- Sicherheitsanforderungen machen es deutlich leichter, sichere Software zu bauen
- Sicherheitsanforderungen sind in der Verantwortung des Kunden
- Wichtig: explizite Anforderungen beschreiben
- Mit testbaren Akzeptanzkriterien
- Lebendes Dokument!

Sicherheitsanforderungen: oft vernachlässigt, dabei sehr nützlich!

Prof. Dr. Sachar Paulus
Fachhochschule Brandenburg

OWASP
The Open Web Application Security Project