Open-Source Communities

Sicherheit bei Open Source Projekten

Gruppe 18
Vorlesung Digitale Nachhaltigkeit 2022

14./21. Dezember 2022

Paco Eggimann
Flavio Gerber
Tobias Brunner

Forschungsstelle Digitale Nachhaltigkeit
Institut für Informatik
Universität Bern

UNIVERSITÄT BERN

Agenda

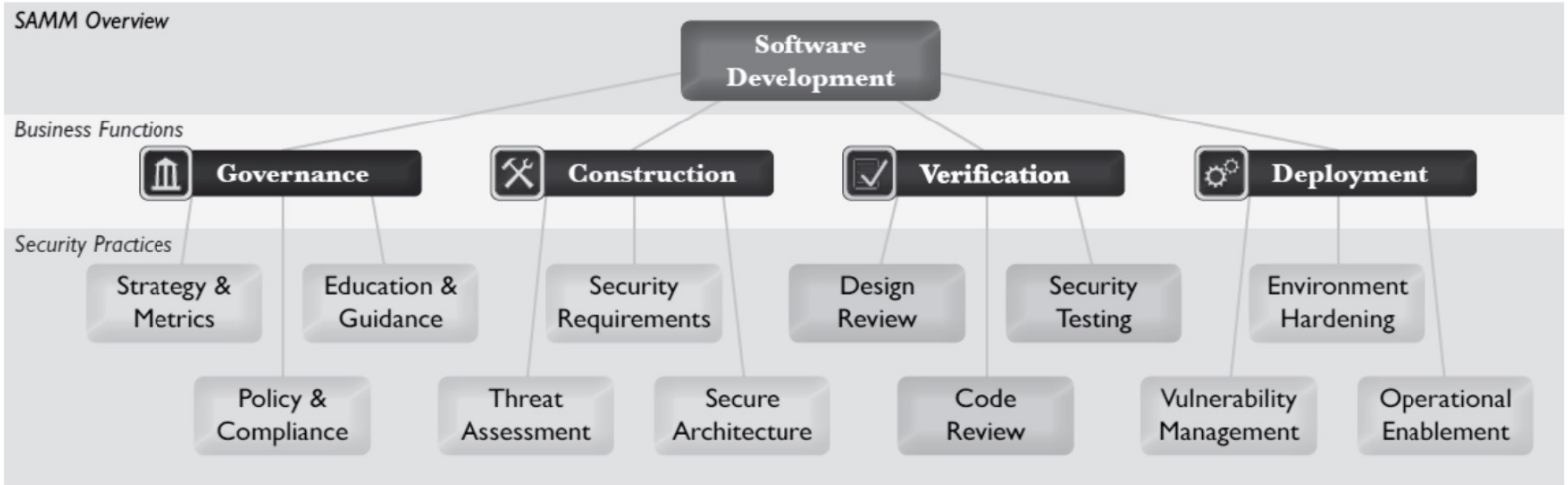
1. **WISSENSCHAFTLICHER TEIL**
2. PRAKTISCHER TEIL
3. PERSÖNLICHES FAZIT

Software security in OSS

«Given enough eyeballs, all bugs are shallow»

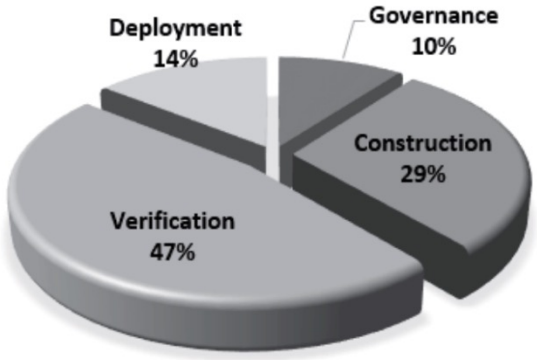
- Eric S. Raymond

Software Development: Security



Software security in open source development

- Auswertung von **42 Publikationen** im Hinblick auf die Sicherheitsbereiche der ausgewählten Studien
- Einzigartige Merkmale der OSS (z.B. gemeinschaftsbasierte, verteilte Entwicklung, Online-Informationsaustausch usw.) tragen zur **hohen soziotechnischen Komplexität der OSS Sicherheit** bei



Shao-Fang Wen (2017) Software security in open source development: A systematic literature review

UNIVERSITÄT BERN

Software security in open source development

- **Verification**
  - Schwachstellen im Entwurf werden sich bei der Codeüberprüfung oder den Sicherheitstests zeigen, wenn sie nicht früher entdeckt werden
- **Construction**
  - Sicheres Systemdesign
- **Deployment**
  - Bei OpenSource fehlt die Unternehmensführung
- **Governance**
  - Bei OpenSource ist mangelndes Sicherheitswissen verbreitet

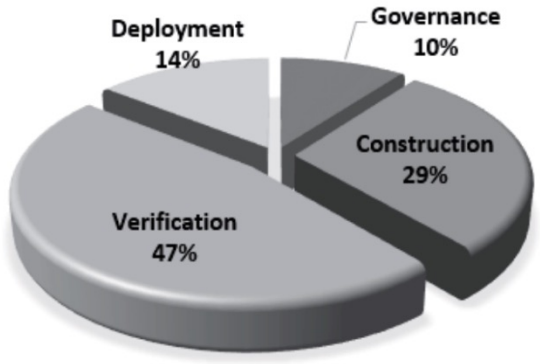
Category	Subcategory	Publications
Governance	Strategy & Metrics	[28, 38, 60, 67]
	Policy & Compliance	[67]
	Education & Guidance	n/a
Construction	Threat Assessment	[14]
	Security Requirement	[22, 40, 58]
	Secure Architecture	[9, 11, 12, 15, 16, 33, 40, 47, 55, 58]
Verification	Design Review	[27]
	Code Review	[1-3, 9, 10, 12, 24, 25, 41-43, 48]
	Security Testing	[16, 17, 30, 34, 45, 46, 49, 61, 64, 67]
Deployment	Vulnerability Management	[4, 6, 52, 54, 63]
	Environmental Hardening	[7]
	Operational Enhancement	[5]

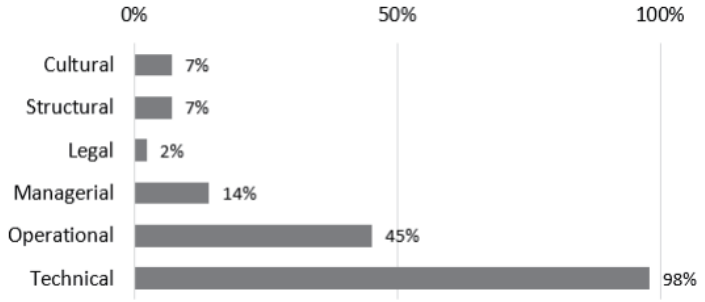
Shao-Fang Wen (2017) Software security in open source development: A systematic literature review

UNIVERSITÄT BERN

Software security in open source development

- **Construction & Verification** werden mit **grösserem Interesse** Untersucht als die anderen beiden Bereiche
- Studien, die sich auf die Entwicklung konzentrieren, sind technisch orientiert und **vernachlässigen** häufig **soziale Aspekte**
- **Mangelndes Wissensmanagement** im Bereich der OSS-Sicherheit





Shao-Fang Wen (2017) Software security in open source development: A systematic literature review

UNIVERSITÄT BERN

Agenda

1. WISSENSCHAFTLICHER TEIL
2. **PRAKTISCHER TEIL**
3. PERSÖNLICHES FAZIT

Puzzle ICT: Verification

- Security Abteilung

- Überprüfung der Software vor der Bereitstellung
- Überprüfung der Software im laufenden Einsatz
- Untersuchung von Sicherheitsbedrohungen

Puzzle ICT: Construction

- Die Verwendung bekannter und bewährter Frameworks mindert Sicherheitsrisiken
- Code-Reviews mit der Sicherheitsabteilung in späteren Phasen der Entwicklung

UNIVERSITÄT BERN

Puzzle ICT: Governance

- Regelmässige Sicherheitsschulungen
- Vorhandenes Knowhow wird in allen Stages des Developements eingesetzt
- Fehlerkultur

Puzzle ICT: Deployement

- Eigene Abteilung für deployement
- Enge Zusammenarbeit mit Securityabteilung
- Verwendung von «proven» Frameworks
  - Openshift

UNIVERSITÄT BERN

Agenda

1. WISSENSCHAFTLICHER TEIL
2. PRAKTISCHER TEIL
3. **PERSÖNLICHES FAZIT**

UNSER FAZIT

- With great power comes great responsibility
- OSS leichtes Ziel, wenn es ungeschützt bleibt (offener Code)
- Sicherheitsrichtlinien während des gesamten LifeCycle der Softwareentwicklung
- Open vs. closed source:
  - Sicherheitsstandards & Best Practices bester Ansatz für robuste Software