



# Open Source Contributions & Security

## Der Weg zu einer Strategie

Martina Götz & Christof Walter | SAP SE  
September, 2023

PUBLIC



# Sprecher



**Martina Götz**

OSS Security Governance Owner  
Product Security Code Governance



**Christof Walter**

Security Engineer  
Security Validation

# Motivation

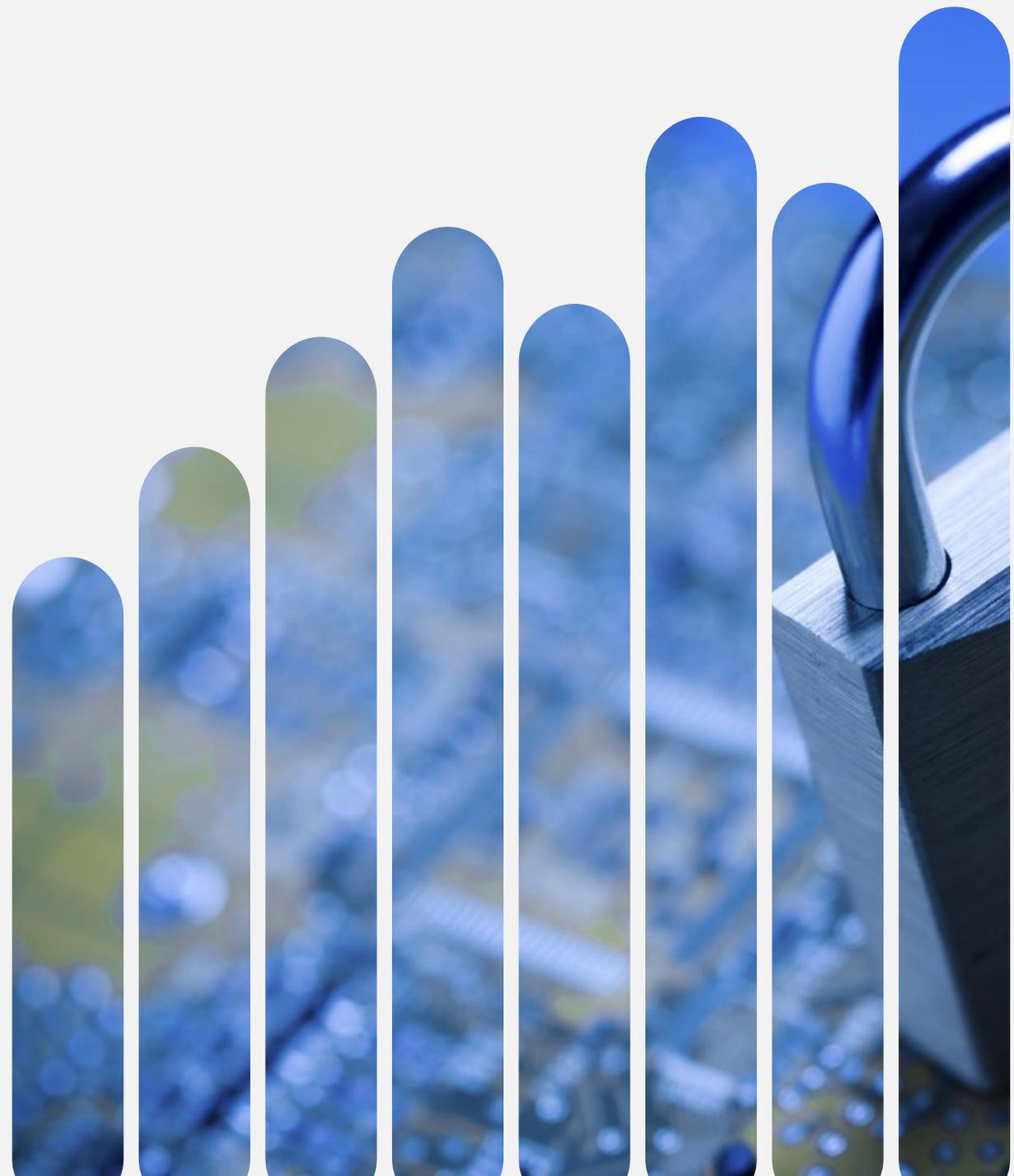
**Nutzung OSS**



**OSS-Rolle**



**Sicherheit**



# 3 wesentliche Szenarien

- Mitarbeitende = **Contributor**

- Mitarbeitende = **Maintainer**

- Firma = **Publisher** einer Open Source Library und **Hauptmaintainer**

# OSS ⇔ eigener Code?

OSS Issue



Firmenpolicy

Findings

Keine Findings

Scary

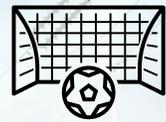
Contribution

Policy

**KEINE ÜBERNAHME-GARANTIE**



...?



Gibt auf

Contribution **akzeptiert**

Security Fix **abgelehnt**

Contribution **akzeptiert**

Security Fix **akzeptiert**

# Mitarbeitende = Contributor

**KANN**

Security für  
eigene  
Contribution

Code Scan

Security  
Fixing

Security  
Community

# Mitarbeitende = Maintainer

Firma übernimmt mehr Verantwortung,  
insbesondere für Security

## Soll

- ✓ Contribution auf Security prüfen
- ✓ Keine neuen Issues akzeptieren
- ✓ Code regelmäßig prüfen
- ✓ Abhängigkeiten aktualisieren

# Firma als Publisher/ Hauptmaintainer

Trägt Hauptverantwortung, incl. Sicherheit

## MUSS: Sicherheitspolicy

- ✓ Anwendung passender Tools
  - ✓ Abhängigkeiten aktualisieren
  - ✓ Analysieren & Fixen
  - ✓ Contributions absichern
- ✓ OSS wie eigenen Code behandeln
  - ✓ Regelmäßig und zeitnah
  - ✓ Transparenz

# Cyber Resilience Act

IT Sicherheit für Hard-/ Software  
(Cybersecurity Risk Assessment)

## OSS-Regulierung

- 🔔 Formulierungen und Definitionen
- 🔔 Beteiligung OSS Communities
- 🔔 Kommerzielle Nutzung

**Cyber  
Resilience  
Act**

European  
Commission

# CRA – Folgen und Gefahren

- 🚨 **Überregulierung & Bürokratie**
- 🚨 **Haftung und Due Diligence**
- 🚨 **Rollen**

## Auswirkungen

- 🚨 **Schaden am OSS Ökosystem**
- 🚨 **Digitale Souveränität**
- 🚨 **Gefahr für Innovation und Wertschöpfung**



# CRA – Schlussfolgerungen

## Allgemein

- ✓ **Kommerziell- gewinnorientierte Nutzung (Downstream)**
- ✓ **Einbindung OSS Communities, z.B. OpenSSF**
- ✓ **Hilfestellungen**

## Strategisch-kommerziell

- ✓ **Contribution-Modell wählen/ prüfen**
- ✓ **Vernetzung mit OSS Communities & Behörden**
- ✓ **Regularien ↔ Policies, Trainings, Unterstützung**
- ✓ **Transparenz**

# CRA – Schlussfolgerungen (strat.-komm.)

**Sich trauen**  
Schwachstellen  
selbst fixen

**Nutzen statt Angst**  
Starkes OSS  
Ökosystem  
anstatt IP Angst

**Aktivere Mitarbeit**  
Mitarbeitende zu  
aktiven Contributoren  
entwickeln

**Investition (1)**  
Policies, Regelungen  
und Hilfestellungen  
bereitstellen,  
Verordnungen  
begleiten

**Investition (2)**  
Beschäftigungszeit für  
Contribution  
und Budget für  
Community-  
Engagement (onsite)

**Transparenz**  
(1) integrierter  
Open Source/ SBOMs,  
(2) Schwachstellen  
(3) Meldungen an  
Meldeüberwachungs-  
behörden

# Zusammenfassung

## KANN

✓ **Contributer können Sicherheit verbessern**

## SOLL

✓ **Maintainer sollen Sicherheit verbessern**

## MUSS

✓ **„Publisher“ müssen Sicherheit verbessern**

---

## OSS Security Policy & Transparenz



# Danke für Ihre Aufmerksamkeit

**Fr. Martina Goetz**

SAP SE

Dietmar-Hopp-Allee 16

69190 Walldorf, Germany

Mail: [martina.goetz@sap.com](mailto:martina.goetz@sap.com)

Phone: +49 6227 7 48986

**Hr. Christof Walter**

SAP SE

Dietmar-Hopp-Allee 16

69190 Walldorf, Germany

Mail: [christof.walter@sap.com](mailto:christof.walter@sap.com)

Phone: +49 6227 7 67464