

☐☐ Manipulation durch Mitwirkung: Sicherheitsrisiko Social-Engineering im Open-Source-Kontext

Open-Source-Bausteine sind zentrale Pfeiler digitaler Infrastruktur und rücken deshalb auch im Zuge der Souveränitätsdebatte stärker in den Fokus. Als grundlegende Infrastrukturkomponente ist ihre Sicherheit zentral. Open-Source-Projekte haben in Bezug auf ihre Sicherheitslage mindestens eine Besonderheit: Die kollaborative Entwicklung ist einerseits eine Stärke, kann andererseits durch Social-Engineering-Angriffe aber auch als Angriffsfläche ausgenutzt werden. Unser [Fokusbericht 01](#) befasst sich deshalb mit Maßnahmen zur Risikoreduktion von Social-Engineering-Angriffen und den damit verbundenen Herausforderungen.

Social-Engineering als Angriffsmuster

Social-Engineering wird zunehmend als Angriffsmuster gegen digitale Infrastruktur eingesetzt. Dabei werden statt technischer Schwachstellen, menschliche Eigenschaften ausgenutzt, also Menschen getäuscht, um Zugang zu Informationen oder Systemen zu erlangen. Phishing-Mails oder Anrufe von vermeintlichen Enkeln sind Beispiele für Social-Engineering aus dem privaten Raum. Zunehmend treten ähnliche Manipulationspraxen auch in der kollaborativen Softwareentwicklung auf Plattformen wie GitHub, GitLab oder Codeberg auf. Angreifer*innen versuchen dort durch durchaus langwierige und komplexe Täuschungsmanöver Projektzugänge zu erschleichen, um Schadcode einzuschleusen. Spätestens seit dem Angriff auf xz-utils, eine zentrale FOSS-Bibliothek, im Jahr 2024 steht dieses Thema auf der Sicherheitsagenda für Open-Source-Infrastruktur. Unser neuester Fokusbericht befasst sich deshalb mit dem Umgang mit Social-Engineering-Angriffen und den damit verbundenen Herausforderungen. [Den vollständigen Bericht findet ihr hier.](#)

Maßnahmen zum Schutz vor Social-Engineering-Angriffen

Für den Bericht haben wir Gegenmaßnahmen auf unterschiedlichen Ebenen zusammengetragen. Auf Projektebene stehen klare Strukturen, Transparenz und technische Sicherheitsmaßnahmen wie Zugriffskontrollen und Code-Signaturen im Fokus, die durch die sicherheitsorientierte Gestaltung von Entwicklungsplattformen ergänzt werden. Auf der übergeordneten Policy-Ebene spielen Gesetzgebung, Kapazitätsaufbau und Förderprogramme eine zentrale Rolle in der Absicherung von FOSS-Infrastruktur.

Stimmen aus der Community

Um diese Maßnahmen im Kontext des Prototype Fund zu verorten und Stimmen aus der FOSS-Community einzubinden, haben wir Interviews mit durch den Prototype Fund geförderten Projektverantwortlichen geführt und einen Workshop auf einem Chaos-Computer-Club-Event durchgeführt. Neben technischen Maßnahmen wurden soziale Faktoren wie Vertrauensaufbau durch persönliche Treffen, menschliche Fehlbarkeit und unterschiedliche Betroffenengruppen entlang der Softwarelieferkette hervorgehoben. Zugleich wurden Ressourcenknappheit und der Bedarf an stärkerem politischen und wirtschaftlichen Rückhalt als zentrale Herausforderungen benannt.

Abwägungen für FOSS-Ökosysteme

Aus unterschiedlichen Perspektiven zeigt sich, dass Social-Engineering-Angriffe in einem komplexen, heterogenen und vor allem sozialen FOSS-Ökosystem stattfinden. Während viele Maßnahmen einen formalisierten und prozeduralen Ansatz verfolgen, wird insbesondere in Interviews und im Workshop deutlich, dass Sicherheitsmaßnahmen vielversprechend sind, wenn sie die soziale Beschaffenheit des FOSS-Ökosystems und die Bedürfnisse der Beitragenden berücksichtigen. Darüber hinaus erhöht ein gesundes Ökosystem auch die Resilienz von Projekten, die in ebendiesen entstehen. Veranstaltungen in Präsenz können beispielsweise den persönlichen Vertrauensaufbau zwischen Beitragenden und Maintainer*innen stärken. Die ohnehin zentrale Finanzierungsfrage im FOSS-Bereich verschärft sich dabei zusätzlich angesichts strukturell begünstigter und häufig besser finanzierten Angreifer*innen.

Nach prominenten Angriffen und damit steigender Sensibilität für Social-Engineering-Angriffe haben zwar einige Akteur*innen begonnen Gegenmaßnahmen zu ergreifen, da bei Social-Engineering der kollaborative Kern von FOSS-Projekten angegriffen wird, ist der Umgang mit dieser Bedrohung jedoch ein Balanceakt zwischen Offenheit und Sicherheit. Dieser erfordert eine hohe Sensibilität für die Besonderheiten von FOSS-Projekten, ausreichende Ressourcen und vor allem ausreichendes Bewusstsein und politischen Willen, digitale Open-Source-Infrastruktur zu sichern.

[Zum Fokusbericht](#)

[Zum Fokusbericht](#)

