Wie sicher ist die Kommunikationsplattform *Consul?*

Quelle: https://www.mehr-demokratie.de/themen/beteiligungs-software-consul/

Von *Eduard Meßmer*, Dezember 2019

Die Plattform *CONSUL* (auch: „*Consul Democracy"-Projekt*) ist grundsätzlich gut aufgestellt hinsichtlich Transparenz, Open-Source und Beteiligung — aber wie bei jeder Software gilt: Die tatsächliche Sicherheit hängt stark von Betrieb, Konfiguration und Umfeld ab.

Es folgt eine Zusammenfassung, was für die Sicherheit spricht, wo mögliche Risiken liegen.

Was spricht für eine gute Vertrauensbasis und hohe Sicherheit ?

- CONSUL ist Open-Source unter der Lizenz AGPL v3 und der Quellcode ist öffentlich verfügbar[1].

- Gute Reputation & breite Nutzung[2]: Consul wird in größeren Umgebungen eingesetzt (z. B. bei großen Firmen) — das spricht dafür, dass sie ausreichend geprüft und skaliert ist. Nutzer- und Einsatzbeispiele (z. B. für Bürgerbeteiligung, Abstimmungen, Vorschlagswesen) zeigen, dass sie funktional etabliert ist[3], denn sie wird weltweit in vielen Städten/Regionen verwendet („über 250 Städte und Regionen" laut Betreiberseite[4]).

- Es wird ausdrücklich gesagt, dass die Plattform in „customisable and secure setups protecting privacy" eingesetzt werden kann[5].

  Viel Ausstattung zur Absicherung und Steuerung

- Es gibt ein ACL-System (Access Control Lists) bzw. Rollen-/Policy-System, mit dem kontrolliert wird, wer welchen Service ansehen oder ansprechen darf.

- CONSUL unterstützt Multi-Cloud und hybride Umgebungen — was wichtig ist, wenn Dienste über verschiedene Netzwerke verteilt sind und man trotzdem Sicherheits-Standards einhalten will.

- Die Plattform bindet gemäß Dokumentation Themen wie Zugänglichkeit („WCAG II") ein, was für Teilhabe und Vertrauenswürdigkeit spricht[6].

---

[1] Github, https://github.com/consuldemocracy/consuldemocracy/tree/master/.github
[2] Hashi Corp: https://www.hashicorp.com/en/products/consul
[3] Observatory of Public Sector Innovation, https://oecd-opsi.org/innovations/consul-project
[4] Hashi Corp, a.a.O.
[5] Aarhus University, CONSUL, https://projects.au.dk/infrapublics/civic-communication/civic-tech/consul
[6] PartiCipate, Platforms for digital participation, https://participation.digital/platforms-for-digital-participation/

Mögliche Schwachstellen bei Kommunikationsplattformen

- Zwar ist der Code öffentlich, maßgeblich sind jedoch Betrieb und Hosting Wenn die Plattform z. B. auf unsicheren Servern läuft, ohne Verschlüsselung oder ohne Zugriffskontrollen, dann sinkt die Sicherheit stark.
- Die Plattform bietet viele Module (Vorschläge, Abstimmung, Mitarbeit) — je mehr Funktionen, desto mehr Angriffsfläche (z. B. XSS, SQL-Injection, unzureichende Authentifizierung) existieren könnten.
- Datenschutz: Wenn personenbezogene Daten (z. B. Nutzerprofile, Login-Daten) verarbeitet werden, muss geprüft werden, wie die Plattform und der Hosting-Betrieb datenschutzkonform ist (z. B. DSGVO in der EU).
- Abstimmungs-/Beteiligungsprozesse: Wenn vertrauliche oder bindende Entscheidungen getroffen werden, müssen die Mechanismen (z. B. Authentifizierung, Nachvollziehbarkeit, Manipulationsschutz) klar geprüft werden. Auch Open-Source hilft, aber ersetzt nicht Betriebskontrollen.
- Updates & Wartung: Open-Source heißt nicht automatisch: „immer sicher". Der Betreiber muss dafür sorgen, dass Sicherheits-Patches regelmäßig eingespielt werden.
- Lokale Anpassungen: Wenn die Plattform stark angepasst wird (z. B. durch eigene Module oder Integration mit Drittsystemen), kann Sicherheit dadurch sinken, wenn Anpassungen nicht ausreichend geprüft sind.

Prüfsteine für Kollaborationsplattformen

Hosting und Infrastruktur

- Wird die Plattform auf sicheren Servern betrieben (z. B. in der EU, verschlüsselt via HTTPS, aktuelle Betriebssystem- und Softwareversionen)?
- Sind regelmäßige Backups, Monitoring und Logging vorhanden?
- Wer hat Zugriff (Admins, Entwickler)?
- Wie sind die Rechte vergeben?

Authentifizierung & Nutzerverwaltung

- Wie wird der Login geregelt? Gibt es starke Passwortrichtlinien, ggf. Zwei-Faktor-Authentifizierung?
- Wie anonym oder pseudonym sind Nutzer? Involviert die Plattform echte Personeninformationen, und wie wird damit umgegangen? (Die Plattform erlaubt u. a. proposal / voting)[7]
- Wie werden Rollen/Permissions gehandhabt? Wer darf was?

[7] PartiCipate, a.a.O.

Daten- & Datenschutz

- Welche Daten werden gesammelt (z. B. Name, E-Mail, IP-Adresse)? Wie lange werden sie gespeichert?
- Gibt es eine Datenschutzrichtlinie („Privacy Policy“)?
- Werden Daten verschlüsselt übertragen (TLS) und sind sie im Ruhezustand geschützt?
- Ist das Hosting-Land relevant (z. B. EU vs. Drittstaat)?

Abstimmungs- und Beteiligungsprozesse

- Wird sichergestellt, dass Beiträge/Abstimmungen authentisch sind und nicht manipuliert werden können?
- Sind die Prozesse transparent (z. B. wie viele Stimmen, wer hat teilgenommen, wie wurde ausgezählt)?
- Gibt es auditierbare Logs oder Mechanismen für Nachvollziehbarkeit?

Software-Wartung & Community

- Wie aktiv ist das Projekt (neue Releases, Sicherheitsupdates)?
  (Das Repository zeigt viele Commits[8])
- Gibt es eine Community, die Sicherheitslücken meldet und behebt?
- Wenn eigene Anpassungen gemacht werden: Gibt es Code-Reviews, Testing?

Zugänglichkeit & Usability

- Ist die Plattform barrierefrei und inklusiv, sodass möglichst viele Nutzende erreicht werden (auch relevant für Vertrauen und Legitimität)?
- (Sie erfüllt z. B. WCAG II laut Analyse)[9].
- Gibt es klare Information an die Teilnehmenden, wie ihre Daten verwendet werden?

Bekannte Sicherheitsvorfälle

Obwohl *CONSUL* weltweit genutzt wird, sind in den großen CVE-Datenbanken[10], Sicherheitshinweisen oder sonst im Netz keine öffentlich dokumentierten Störfälle adressiert (z.B. Datenleck, Manipulation von Abstimmungen … etc.). Die Tatsache, dass keine CVE-Einträge direkt für *CONSUL Democracy* gefunden wurden könnte jedoch auch bedeuten: Es wurden Schwachstellen bisher nicht als offizielle CVE´s gemeldet oder dokumentiert – oder sie waren weniger gravierend bzw. intern behoben.

---

[8] GitHub+1, a.a.O.

[9] PartiCipate, a.a.O.

[10] Bei CVE (Common Vulnerabilities and Exposures) handelt es sich um ein internationales Nummerierungs- und Klassifikationssystem für bekannte Sicherheitslücken in Software oder Hardware. Jede dokumentierte Schwachstelle, die öffentlich bekannt gemacht wird, erhält eine eindeutige CVE-Kennung (z. B. *CVE-2024-12345*). Diese Kennung erlaubt es, dieselbe Sicherheitslücke weltweit einheitlich zu identifizieren und zu referenzieren — etwa in Sicherheitsberichten, Updates, Firewalls oder Patch-Management-Systemen.

Es ist bei Beurteilung der Sicherheit der Unterschied der Software zu beachten, namentlich ob es sich um „*Consul*“ beispielsweise von HashiCorp handelt oder um „CONSUL Democracy“. Manche verfügbare Schwachstellen beziehen sich nicht auf Ihre Plattform. Man darf also nicht ohne Weiteres von Schwachstellen bei HashiCorp Consul auf CONSUL Democracy schließen.

Fazit

Die Plattform *CONSUL* ist sehr gut einsetzbar für Beteiligung und Kommunikation mit starken Grundlagen — insbesondere da sie Open-Source ist, viele Einsatzfälle hat, und explizit „secure setups” nennt.

Aber: sie ist **nicht automatisch sicher** — Sicherheit hängt vom Betrieb, von Installation, Hosting, Konfiguration und der Begleitung ab.

Dennoch erfordert im Zusammenhang mit Sicherheitsaspekten Open-Source Software aktive Betrieb und Pflege.

Beim Einsatz ist zu beachten: Jede Umgebung, in der die Software läuft (Server, Hosting, Netzwerk, Benutzerverwaltung, Plugins) könnte zum Schwachpunkt werden.

Wer die Plattform einsetzt, sollte also besonders auf den sicheren Betrieb achten (Updates, Zugangskontrolle, Hosting-Sicherheit, Audit-Logs) — und sich nicht darauf verlassen, dass „weil bisher nichts passiert ist“ automatisch alles sicher ist.