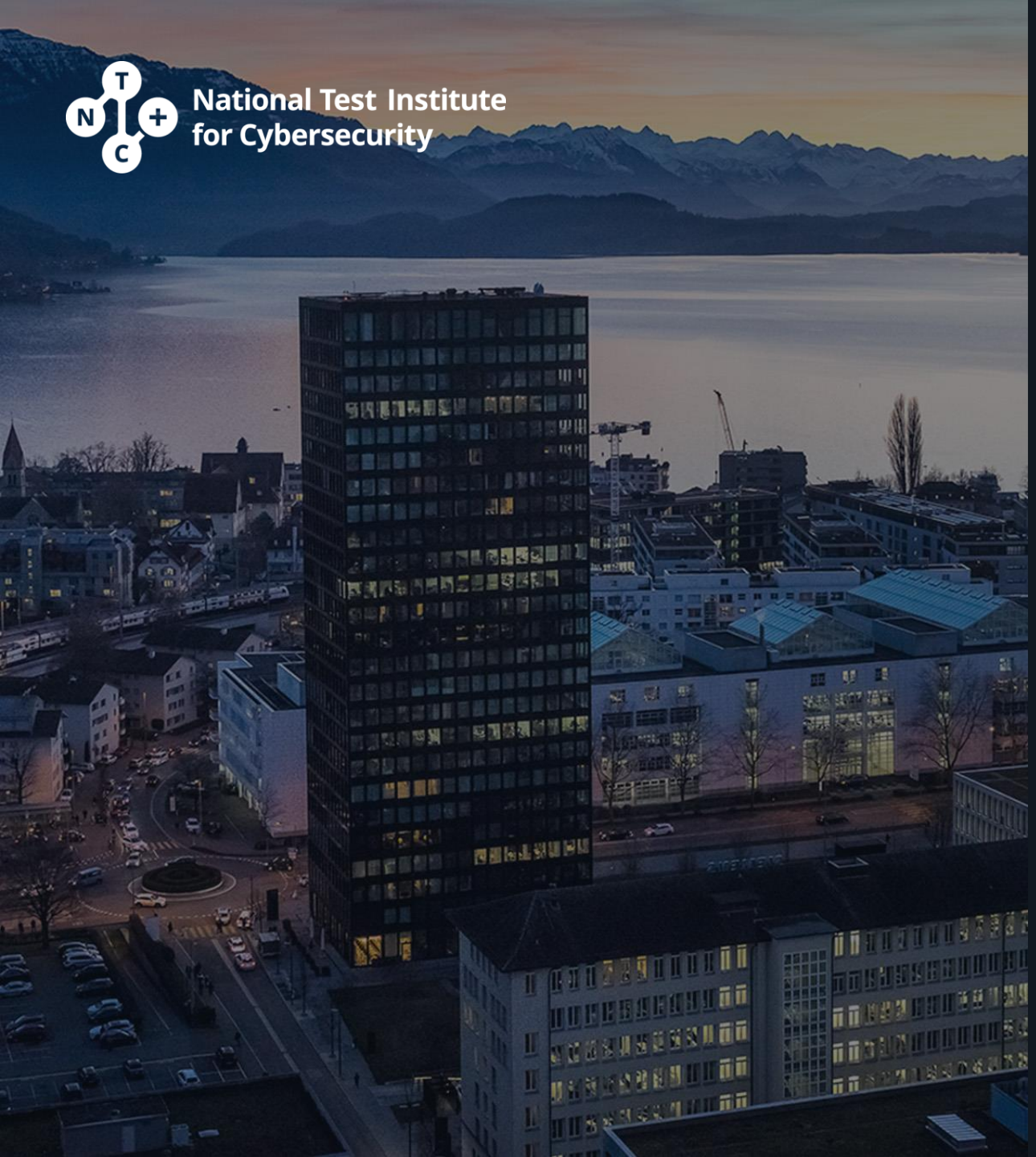


Security in Open Source - Insights of the NTC

Fabio Zuber, 04.06.2025

National Test Institute for Cybersecurity

Fabio Zuber

- Penetration Tester
- Background as Inner Source Developer

Mehrere Swisspass-Ko

Von Keystone-sda / cwi, 20. Mai 2025 um 11:

SECURITY SBB ALLIANCE SWISSP

Foto: Swisspass

Seit Anfang Jahr wurden in Konten von Hackern missb durch Phishing erlangt.

Angriff auf Mail-Konto von Betreiber in Birr

Von Keystone-sda / paz. 15. Mai 2025 um 11:19

SECURITY CYBERANGRIFF ENERGIE KR

PRISMECS

Reservekraftwerk in Birr. Foto: zVg

Im Namen des Schweizer Gesc versandt. Laut Bund waren die Angriff betroffen.

Hacker erbeuten Ges Westschweizer Rönt

Von Philipp Anz, 22. April 2025 um 11:10

SECURITY CYBERANGRIFF GE

Foto: Getty / Unsplash+

Nach einem Cyberan kopiert wurden. Eine abgelehnt.

Cyberangriff trifft Swiss Life und Pensionskassen

Von Christian Wingeier, 24. März 2025 um 11:55

SECURITY SWISS LIFE CYBERANGRIFF CYBERCRIME FINANZINDUSTRIE SCHWEIZ

Der Hauptsitz von Swiss Life in Zürich. Foto: Swiss Life

Rund 60 Pensionskassen dürften von einem Datenleck betroffen sein. Schuld daran ist ein Angriff auf einen externen SMS-Provider, der Zwei-Faktor-Identifizierungen anbietet.

https://hub.ntc.swiss

We test what is otherwise not tested.

Nationales Testinstitut
für Cybersicherheit

- Non-profit registered association located in Zug
- Public funding
- «We test what is otherwise not tested.»

Initiative projects

Customer projects

- Team of permanently employed specialists

- «We **test** what is otherwise not tested.»

  ↳ **= Technical Security Analysis**

  aka Hacking or Penetration Test

Open Source Software

OSS user

96.6%

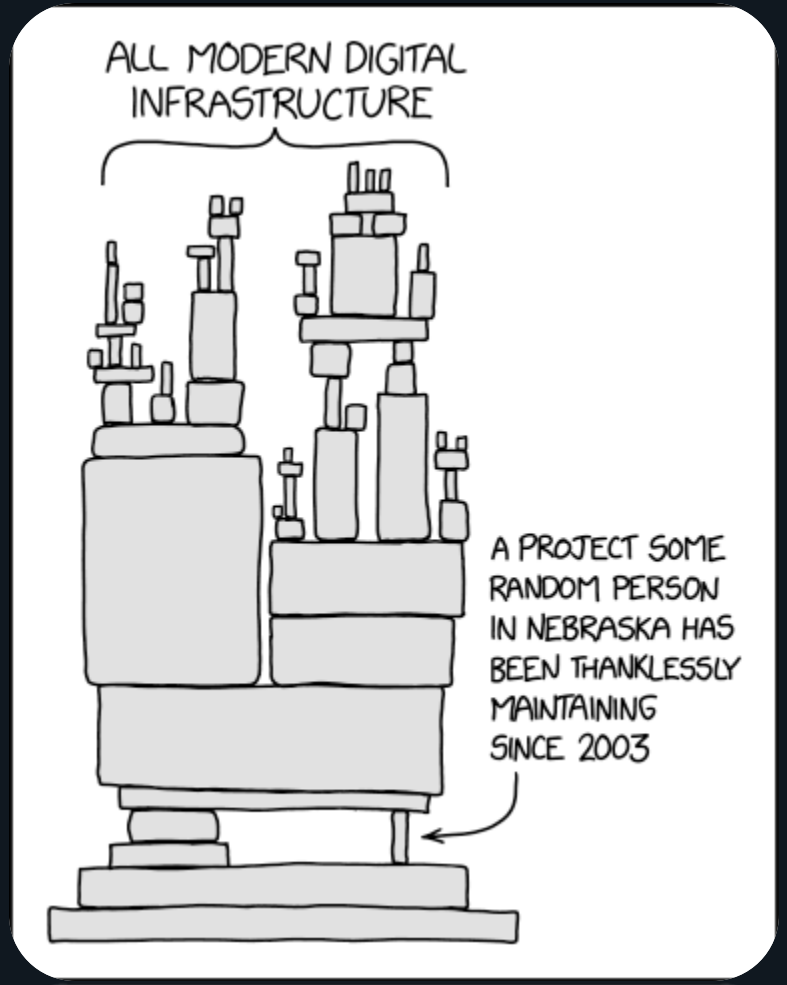
Heavy OSS user

49.4%

National Test Institute for Cybersecurity

Source: Open Source Studie 2024

Open Source Software



National Test Institute for Cybersecurity

https://xkcd.com/2347/

Vulnerabilities

Log4Shell in Log4j (CVE-2021-44228)

regreSSHion in OpenSSH (CVE-2024-6387)

Backdoors
(or Bugdoors)

XZ Utils Backdoor (CVE-2024-3094)

CocoaPods Dependency Manager (CVE-2024-38368)

Relevant Projects

Xamarin

Remote Code Execution using Server Side Template Injection — High
GHSA-q37x-qfrx-jcv6 published on Mar 12 by gmazoyer

Open redirection using the return_url parameter — Low
GHSA-f4mf-5g28-q7f5 published on Mar 12 by gmazoyer

Stored XSS on router page — Moderate
GHSA-fmf5-24pq-rq2w published on Mar 12 by gmazoyer

Send ideas to:

fabio.zuber@ntc.swiss

ntc.swiss/contact

Fabio Zuber

Penetration Tester | BSc Information and Cyber Security

National Test Institute for Cybersecurity

«There is no silver bullet»

Ressources for Maintainers

Compensation and recognition

Security *Audits*

Tools and Know-how

SBOM

Software Bill of Material

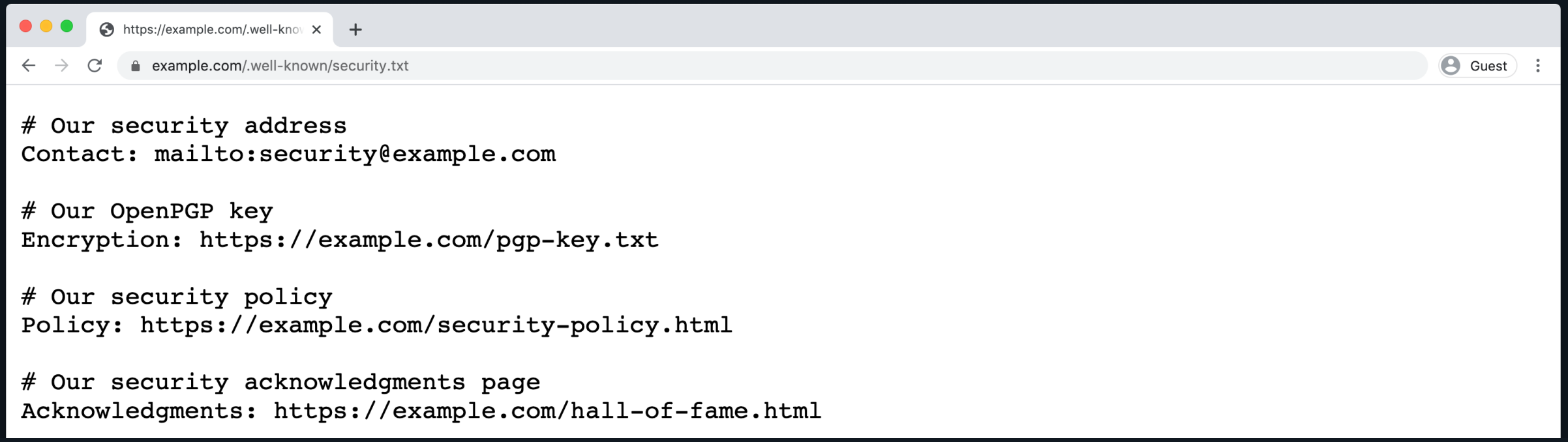
«There is no silver bullet»

Evaluate the whole attack surface

«Secure by default»

CI/CD pipelines with security checks

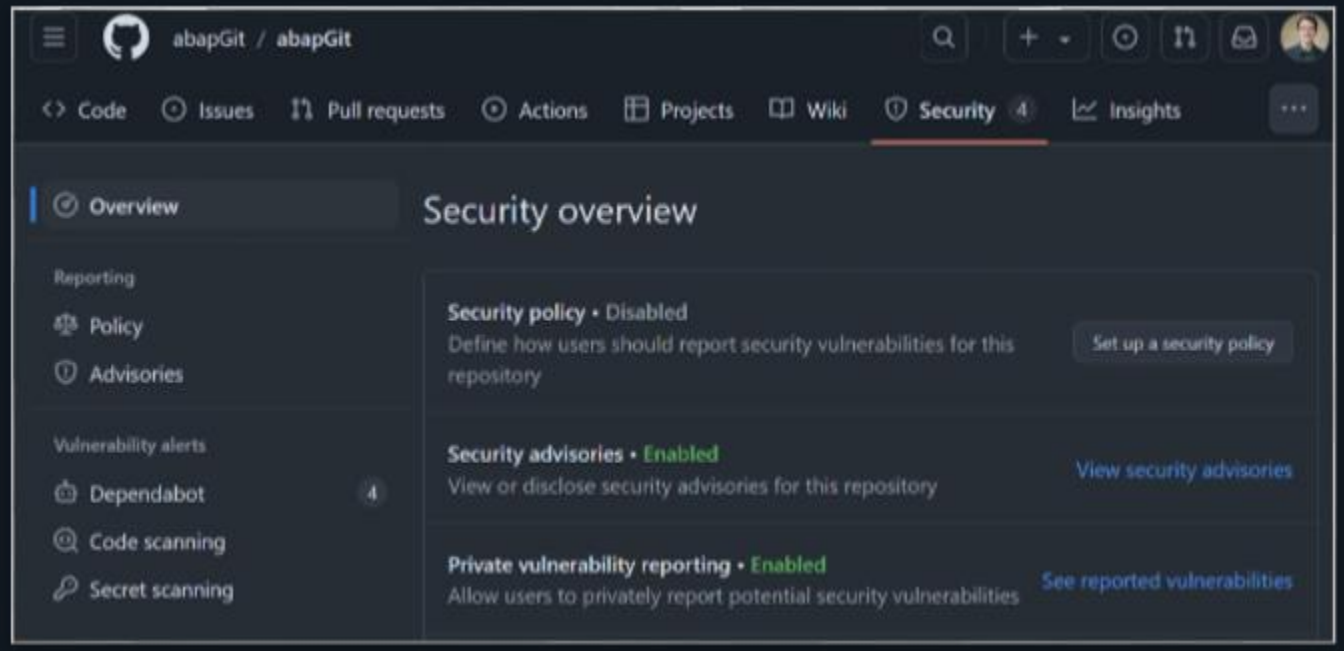
Contact for Security Issues



https://securitytxt.org/

Contact for Security Issues

SECURITY.md



https://github.com/

Fabio Zuber

Penetration Tester

National Test Institute for Cybersecurity NTC

ntc.swiss

National Test Institute for Cybersecurity

Thank you for your attention!