eduGAIN Security Team

Daniel Kouril

63rd TF-CSIRT Meeting

May 28, 2021

eduGAIN

72 Identity Federations

4000+ Identity Providers

3000+ Service Providers

30 milion user identities

Incident Response in eduGAIN

- Individual federations differ in expertise and resources available, policies/procedures, and links to their constituency
- Even more fragmented on level of IdPs/SPs
- Potentially huge impact of security incidents
- eduGAIN Security Team formed as global IR capability

eduGAIN Security Team

- Established as part of the operational teams
- Security help/coordination/consultation for eduGAIN federations and individual participants
- Core composed of a few security experts
  - Sven Gabriel, Daniel Kouril, Romain Wartel
  - IR, coordination, forensics, building community/trust
- Highly interconnected with other infrastructures and orgs in EU, US, APAC
- https://edugain.org/edugain-security/

Recent activities

- eduGAIN Security Incident Response Handbook
  - roles and responsibilities in the IR process
- Communication challenge performed
  - Check of security contacts of federations
  - Dec 15-23 2020, 28 federations contacted
- Sharing threat intel
  - Notifying relevant parties, procedures being discussed
- Responding to incidents
- Establishment of eduGAIN Security WG

Conclusions

- eduGAIN has dedicated IR capabilities in place
- Internal/external procedures are constantly developing
- Continuing to build trust relationships with the community and constituency