April 26, 2018

Attending: Tom, Scott, Romain, Hannah, Pål, Shannon, Uros, Francisco, Alan, Dave, Brett

Since Niels can't join us today, I thought we'd focus on the AARC DNS3.2 Security Incident Response Procedure and return to the registry after we've heard from Niels.

Proposed agenda

1. Agenda bash
2. AI review
3. Plans for "Federated Security Incident Response Procedure"
    a. Discuss potential objectives of this REFEDS doc:
        i. Provide Incident Response (IR) templates and concrete procedures
            1. CISO brought into an IR without any federation background
        ii. Assign IR roles & responsibilities
            1. Prescribe a central coordinating role at eduGain level
            2. Roles for national federation operators
            3. Established CSIRTs, somehow
            4. IdP/SP/proxy operators, especially those at smaller organizations who need not be security professionals
            5. Reporting on actual incidents
        iii. Requirements of IR Plans and contacts for eduGain federations
            1. Provide examples or templates
        iv. Identify technical and functional requirements for sharing confidential information associated with IR
            1. Among those managing an incident
            2. For IdP, SP, or federation operators to proactively notify of troubling developments
            3. What should, should not be shared
            4. How to share which type of info with whom
        v. Prescribe tabletop testing procedures
            1. Recognize that there will be a layered approach to this, so the prescription may be to suggest who should start out how
            2. Good models for tabletop testing
            3. Sample scenarios to test
            4. Venue/location at which to share lessons learned from tabletops and from actual incidents
        vi. White paper-level material on IR in a federated context
            1. Maybe not … keep focused on the practical side. But …
            2. We expect that some people will get incorporated into an IR who have no federation orientation.
            3. Perhaps in an appendix, a secondary objective of the paper

        vii. Other?

    b. Gdoc copy of the AARC deliverable
    c. Take a moment to scan table of contents, skim a bit. Any immediate reactions?
    d. Homework: read and make notes or comments in the gdoc before next WG meeting. Which material should be carried into the REFEDS paper?
        i. Written for AARC audience so some terminology is rather “advanced”, for those with deep experience.

4. Time permitting, review tasks in the work plan to satisfy ourselves that we’re focusing on the right things for now

- https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting
- REFEDS survey: please report on your tabletop testing procedure for this year. If you didn’t, why not?
- Example of REN-ISAC sharing roles.
- https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-sending-incident-reports-overseas Sending Security Data overseas (GDPR)
    - Perhaps ask Andrew to review and comment on our draft doc