20210302 - Planning Meeting for eduGAIN SWG

Attendees:

Notes:

Chair: Davide proposed to have 2 chairs. 1) Sven Gabriel and 2) FedOperator
Casper shared https://wiki.geant.org/display/eduGAIN/Working+Groups
For now no fixed term for chairs.
Chris: in scope for this group -> baseline recommendations.
Pål: narrow down, otherwise we end up doing everything and therefore nothing.
Sven: long term and short term goals. Reflect on the goals. Communication infrastructure to contact the federation operators. Mandate: what is expected from us. Decided by SG.

Davide: Recommendations to the community?
Chris: Do we need an Emergency contact list? This will take time and resources.
Pål: Put eduGAIN SIR on the SG agenda.
Davide: SIR consultation is underway. Passed REFEDS and got approved. No comments received so far. https://wiki.geant.org/display/eduGAIN/Security+Incident+Response+Handbook+Feedback

Received comments from experts during the SIRTFI/REFEDS consultation.
Davide: Two main tasks:
  1. Proposed recommendations to eSG. And how do we enforce the outcomes
  2. Define the function of the Security team. Reactive (incident response) and proactive (awareness campaigns).

Pål: This group could make suggestions on how to communicate effectively with the eSG / FedOps.
Chris: Help the security team to understand what the gaps currently are. What does the security team like to see from the fedops to improve.
Sven: Agree.
Romain: Missing link between fedops, SPs, IdPs and the security team. Security team as an operation tool.
Chris: This group being the ambassador to be ready for incident response? We can create a lot of work for ourselves. What would be the part of the work.
Romain: Nothing specific. Threats to R&E as a whole. Challenges like different infrastructures. One more way to reach out to different levels of the community. eduGAIN one more layer.
Chris: Is it a SOC?
Romain: Not really. This team is mainly reactive. But if there hints of malicious activities the team will act. Coordination and cooperation.
Davide: The team's remit is more or less described in the SIR.
Shannon: Sounds like more bottom-up than top-down. However, he doesn't think we are currently operating this way. This could be one of the tasks/goals this WG could address.
Romain: Try to close the gap between scientific and campus computing.
Terry: Is this something we can help to impact?
Chris: It's rare that we communicate with the community. So this needs to be established.
Romain: #1 priority: provide incident response abilities for eduGAIN.
Sven: The security team has a limited view on what is going on in eG and it's infrastructure. Feedback from this group.
Chris: Emergency preparedness is the big topic.
Davide: Establishing a trusted community channel to the identity federations. These are the initial goals.
Terry: Layered approach. Security team looks at IdFeds. IdFeds look at SPs and IdPs.

Romain: Especially with planned campaigns.

Pal: Hard to balance the number of messages to the end points.

Romain: Send valuable content of high quality. Higher chance that your message will reach the right people.

Chris: Assist with prioritise the types of messages. Help/train the community what is expected of them.

Pal: Risk of losing interest because of overload of information.

Sven: The security team’s mandate should be transparent.

Pal: I need this when I talk to my constituency.

Davide: How will we proceed?

Pal: Suggestion: Security team to come up with some concrete action plan.

Romain: eduGAIN passwords.

Terry: “Layered approach before we send out communications”. Make the community aware.

Sven: Mixing up 2 major problems. Security incident response part and proactive part. We could also think of an opt-in approach for the proactive part.

Terry: What does the team expect to receive as a response?

Romain: The less the better.