20210216 - planning meeting for eduGAIN SWG

Attendees

- Davide Vaghetti - GARR
- Marina Adomeit - SUNET
- Nicole Roy - Internet2
- Shannon Roddy - Internet2
- Pål Axelsson - Sunet
- Wolfgang Pempe - DFN
- Miroslav Milinovic (SRCE / CARNET)
- Daniel Muscat - RicerkaNET /University of Malta
- +1 for list: Chris Phillips (CANARIE)
- Rafal Lawrukiewicz (CANARIE)
- Thomas Bärecke - SWITCH
- Attila László - KIFÜ/eduID.hu
- Nicole Harris - GÉANT
- Maja Gorecka-Wolniewicz (PIONIER.Id)
- Tomasz Wolniewicz (PIONIER.Id)
- Terry Smith (AAF)

Agenda

- eduGAIN Security Working Group set up (see also https://wiki.geant.org/display/eduGAIN/Working+Groups)
    - Aim and Objectives
    - Duration
    - Meetings
    - Decision making process
    - Deliverables
    - Membership & Chair
    - Communication (to cover for people outside the eSG)

Call notes

For communication within the WG - set up mailing list as the first step.

Aim and Objectives

Davide V.: There is eduGAIN security team and SIR, but there is no mandate for the eduGAIN security team, also SIR needs yet to be adopted by the eduGAIN SG.

Chis Phillips: We are in a good position to have resources for eduGAIN security team.

Marina A: eduGAIN SIR recognises the existence of eduGAIN security team.

Nicole H: leaving the instrument out of this - perhaps we can talk first how would federation operators prefer that the information about security incidents or proactive security information is being shared ? What are the issues, what do we need it to be addressed. How do we use edugain security team resources ?

Chris P.: what do we learn from the previous experiences

Nicole R. : supports. With whom does the eduGAIN security team talk to? We can clear out in this working group specific cases.

Chris P: bring up specific proactive campaigns to the WG to agree. These should be also documented for reference for new members, so that they know what to expect.

Nicole H: the heartbleed security incident was difficult to deal with as there was no framework, there was a whole different set of things that can happen when big incidents hit our community. How do we better manage communication and workflow so that we don't have to define this as we go on.

Chris P.: There are also predictable events that can have impact on security that we can work on.

Davide V: The eduGAIN security team also helped gather the security contacts. We need somebody

Marina: we have three types of activities, reactive -> SIR, proactive (information threats, communication channels verification), build a trusted security community in eduGAIN

Chris P: have simulations for resolving security incidents - also feedback on what they did right, and what can be improved. Expectations for such simulations or communication challenges should also be better defined.

Pal A: How will small federations handle situations. We also need to find way that this works for the ones that are understaffed.

Nicole R: could we do a survey?

Nicole H: we could do more discussion and reaching out to people, being careful that we dont create too much work for people. Relation of CSIRT teams and federation operators differs heavily

Nicole R: there are different groups like trusted introducer, research infras etc we can also engage with so that we help as much as possible federation community from different sides

Shannon R: agree that this group could help establish relationships with such groups

Chris P: this group could also help with adoption and application of frameworks that can help increase security such as MFA

Pal: There are a lot of ideas shared now - but we need to focus on priorities or else we will not do anything

Nicole R: would be happy to agree to do one thing at first - and this is to prevent the situation like with leaked credentials notification happen again.Other stuff we can put in a backlog bag

Chris P: Agree for the WG to be like the sounding board

Davide V: composition of the eduGAIN security team - this should be outcome of this wg

Nicole H: membership of the WG - we should define rules of membership for the working group so that we have tight and well defined membership, have the right people in who can really contribute to the work

Action points:

- [x] Davide V. will send doodle invite for the next meeting of the WG - hopefully before the next SG meeting which is in March
- [x] Nicole H. will setup a mailing list
- [x] We should have a draft of the WG charter that defines amongst other things objectives and membership so that we can discuss it at the next call.