20210512 - Planning meeting for eduGAIN SWG

Draft notes:

Attendees: Terry Smith, Davide Vaghetti, Björn Mattsson, Wolfgang Pempe, Sven Gabriel, Attila Laszlo, Russell Ianniello, Nicole Harris, Marina Adomeit, Casper Dreef, Pål Axelsson, Daniel Kouril, Chris Phillips, Shannon Roddy, Romain Wartel, Daniel Muscat

Co-chairs: Sven Gabriel (representing Security Team) & Shannon Roddy (representing eSG)

Both co-chairs were accepted. The charter was accepted.

The Working Group moved from planning to actual state

SheerID incident

Davide explained the eduGAIN leadership sent an official letter to SheerID. A list of federated entities have been shared by SheerID and the Security Team.

This list might not be complete and accurate. Non-federated entities are missing.

The Working Group expressed its surprise about the incompleteness and inaccuracy of the list. One of the problems is that entities don't keep logs longer than a certain amount of weeks and therefor are not able to check if they were affected. eduGAIN doesn't have the ability to filter out a single entity. UKfed could be asked to filter SheerID. Terry asked if there is an alternative for eduGAIN, e.g. InAcademia.

Which options are available to filter out entities in case of an emergency? Important to keep 'trust' in mind. "Why can't I log in" vs "Why must i audit my logs for a compromise after the fact". At the moment there is one option: completely drop a federation's feed.

Work on a 'measured response' in the policy. Chris pointed out this could be an opportunity for SIRTFI adoption. Romain noticed that by design some main elements are missing in the current policy. Sanctions and emergency measures are different things. Both are missing at the moment.

Policy needs to be revisioned. A call for working group will be addressed at the Drop-in Session at 18th May.

Topics proposals

Chris proposed the topic of best security practices in eduGAIN. What do recommendations mean in practise. The group supported the idea.

Davide proposed to identify the missing bits and raise this to the Policy Revision Working Group as well. The Security Team will make its wiki space available of a Best Practise section. eduGAIN Security