20210113 - planning meeting for eduGAIN SWG

Attendees

- Terry Smith - AAF
- Marina Adomeit - SUNET
- Carlos Friaças - FCCN (PT)
- Wolfgang Pempe - DFN
- Shannon Roddy - InCommon
- Donald Coetzee - SAFIRE
- Guy Halse - SAFIRE
- Daniel Kouril - CESNET
- Irfan Hakim - SIFULAN
- Pål Axelsson - Sunet
- Miroslav Milinovic - AAI@EduHr
- Tomasz Wolniewicz - PSNC
- Martin Stanislav - SafeID
- Maja Górecka-Wolniewicz - PSNC
- Esmeralda Pires - FCCN
- Thomas Lenggenhager - SWITCH
- Attila László - eduID.hu
- Casper Dreef - GÉANT
- Barbara Monticini - GARR
- Daniel Muscat - RicerkaNET
- Sven Gabriel - EGI/Nikhef CSIRT
- Licia Florio - GEANT
- Davide Vaghetti - GARR
- Alex Stuart - UK federation
- Chris Philips - Canarie

Agenda

- eduGAIN Security Team Mandate
    - Coordination of inter-federation security incident response - eduGAIN SIR Handbook approval
    - Proactive work - Security threats information sharing
        - Define the process for communications originated at the eduGAIN Security Team and targeted to final entities/federation participants.
- eduGAIN Security Community establishment
- How do we continue working on this - establish an eduGAIN WG?

Call notes

- Davide: Intention to listen to community on role of security team
- In 2020, eduGAIN Security team wrote document: “incident response handbook”. Very good consultation, good feedback. Consolidated handbook has been sent to REFEDS Steering Committee for approval.
- Nicole: it has now been approved by Steering Committee
- Davide thinks main mandate of security team is coordination of incident response; secondary is proactive work like information sharing about security threats.
- Call to group: any other parts to mandate?
    - … your answer here ...
- Building community: eduGAIN steering group (eSG) is delegates and deputies, a similar trusted group is what we have in mind;
- Ends reviewing agenda & opens to floor

Terry: noted lack of communication with eSG, federation operators. Content and branding of communications could be improved.

Pål: comms should not go direct to entity operators; a trust problem

Nicole: is this a flaw within SIRTFI itself? It requires a security contact in metadata.

Pål: SIRTFI is reactive not proactive; there’s a distinction

Signalling in comms to fedops so entity owners have a known trusted contact to contact

Miro: for me, enough to cc federation operators in the same email.

Licia: credentials already compromised, but we thought not appropriate to share [the identifier?] with fedop; we thought maybe a parallel email to fedops?

Davide: identifier & credentials in data dump already

Miro: not guarantee that the credential is for IdP account, could be random twitter with that email identifier. Email address is an attribute from IDP, not controlled by IdP.

Davide: We are taking a similar approach to CERN, REN-ISAC. Re-use of passwords associated with same email identifier.

Miro: [you should put warnings first]

Davide: back to earlier point, we need to review communications

Davide: we heard information received from several points, we must address this

Pål: must have optin/optout

Marina: [first thing about communications]; 2nd is campaigns that are conducted periodically; 3rd, review communications of those campaigns

Davide: we know some communities already review osint

Chris: introduces concept of duty of care for communications under the flag of a particular community. Unclear whether this is GÉANT, eduGAIN, CERN activity.

Davide: CERN & CSIRTS in Europe doing this for eduGAIN; by chance one member of security team is in CSIRT in CERN, and gets such data dumps. Acknowledges concerns.

Licia: should security team have mandate for reactive; or reactive + proactive? We have found that people use the security contact for any security issue, and this appears problematic.

Chris: asserts that a security contact in metadata is similar to abuse@domain within email. We need to help, inform & train these security contacts “these are the benefits you get”. But fedops may not have bandwidth to do this, and not want to get in the way of such training. Ties to Baseline expectations for operating in a federation.

Nicole: clarifies that security contacts can appear separate to SIRTFI assurance-certification ; have extensive [materials on this]. [mechanisms for building trust]. We need more than just saying you are SIRTFI; need to understand & share how these are used.

Davide: how do fedops want to be involved in these communications

Miro: I should be notified, not wanting to be a proxy

Shannon: concrete example of an outsourced IdP who has the security contact & received email. The outsourcing org thought sharing restrictions meant couldn’t be shared with fedop. Re: comms, risk that they imply participating in federations brings this risk

Chris: agrees!

Shannon: not implying against proactive work, but orgs like NIH mandating federation and working with small medical org, who then outsources IdP. Several layers of abstraction. Reiterates all parties must be informed, so fedops can manage perceptions & guide and help.

Chris: A shopping list of requirements would be TLP:GREEN (preferably) or TLP:AMBER; how often will this happen; how fits into framework; numbers or contacts informed.

Davide: Sharing rules for TLP are interpreted differently, for example EGI community established meaning for each TLP colour for that community.

Nicole: clarifying TLP:AMBER should be OK, adding to it is problematic. Note context of TLP:AMBER, for some circumstances could share, others not. SHOULD rfc2119!

Chris: notes that differences in attitude to notification about a security incident varies depends on person receiving information. Busy campus helpdesk may be de-sensitised to this kind of thing, gets hundreds of password reset request per week.

Davide: More than just opt-in/opt-out to communications [per federation rather than per-domain], do you, as fedop, want to use this service?

Chris: I’d use whatever mechanism was presented to me

Davide: if enough consensus in our community would rather have that, than opt-in/opt-out.

Pål: removing security contact from metadata would be a way to deal with this, but problematic

Davide: overloading security contact & removing trust

Marina: opt-out by exception not a general option?

Davide summarises: will keep fedops in loop, will define process, define working group?

Marina: options seem to be: a WG / a couple more of this larger / happy with feedback you’ve given? Notes that eduGAIN SG meeting very busy agenda, need some smaller groups for ideas in development.