20210318 - Planning meeting for eduGAIN SWG

Notes:

Davide opened the meeting and proposed to discuss the action plan prepared by the Security team. (presentation Sven)
Key aspects:
- Support of the governing body

- Support of the parties involved in the security operations

Where to start from?
- DNA3.2
- SIR handbook (currently in consultation)
- Transparency: define roles and responsibilities

Comms in case of incident response: 1) All comms through Federation (proxy model); 2) Fed in CC; 3) Direct comms with eG entities.

Pal: eG not the only interfederation we have. We need to see this wider than eG.

Sven: True, but we need to start somewhere. Build the infrastructure and later coordinate with others.

Daniel: Let each federation decide what works best for them. Option 1 and 2 would be most useful.

Sven: That was the idea. We advise to use 1 or 2.

Daniel: For 2, does the security team have the resources to contact all IdPs?
Sven: Not so much a technical problem, more dependent on how the federation is set up. Some coordination with the federation is required. Especially when the federation has many entities. A lot of communication at the beginning. This will be challenging. The federation will play an important role.
Davide: Pal, what are the benefits for SWAMID to go for 1?

Pal: Our CERT is involved. A hybrid between 1 and 2 might also be an option.
Bjorn: The problem is always to establish trust. SWAMID/SUNET has a well developed trust network. SUNET CERT to establish trust with the entities.
Sven: Including CERTs in CC already some sort of control mechanism. The security team needs to know what is going on. Communication goes in both directions.

Bjorn: In 1 you can build more easily on a trust relationship.

Davide: 1 is the best way to build the relationship between the security team and fedops certs. Question about SIRTFI. What about incident response coordination? Doesn't 1 clash with SIRTFI.

Pal: SIRTFI is for entity to entity, not a central contact.
Attila: Many entities are not expecting to eG directly. In case 2 and 3 direct communications is established. This is a change of the status quo.
Sven: The problem is that you might lose precious time. Communications get slow.
Davide: Unless in case of CoCo infringement or when they contact us directly, eG indeed doesn't talk directly to entities.
Sven: The most important thing for the security team is that whatever route is chosen, this is clear to everyone.

Marina: What if an SP is registered in multiple federations? Which federation preference to apply?

Bjorn: Propose to always start with 1 to jumpstart trust relationship between security team, fedops and entities. After the trust chain is properly established, you can move to 2.

general agreement

Marina: 1 requires a security contact.
Daniel: Could personal data be involved? GDPR sensitive information. For instance the credential dump.
Davide: CERTs/CSIRTs are excluded in case of incident response.

Pal: But we need to be careful.

Daniel: We don't have a CERT or official security team. Would that be an issue if we would go for option 1?
Davide: In that case personal information will normally not be shared. It really depends on the situation.
Pal: Now we are speculating. Again, we need to be careful.

Sven: We need some legal advice here.
Pal: Now we are talking Europe only. This is also why we need to be careful.

Davide: https://www.first.org/blog/20171211_GDPR_for_CSIRTs could be useful.
Shannon: We have a security contact but not a 24/7 team. It really depends on the incident. Security vulnerability is different from a credential dump.

Davide: Conclusion: strong preference for proxy model to establish trust relationship.
One of the first steps is the discussion in the eSG about the SIR handbook. Decision on adopting the SIR handbook and include it in the eG policy set.