Sirtfi Metadata Consultation Followup

15:00 CEST 18/04/2016
Attendees:

1. Andrew
2. David
3. Hannah
4. Heather
5. Jim
6. Nicole
7. Romain
8. Scott
9. Tom

Consultation:
https://wiki.refeds.org/display/CON/Consultation%3A+Managing+Metadata+Extensions

Feedback from Consultation:

1. Andrew - We should address Jim's Open Questions:

    a. What should security contact in metadata contain? – EmailAddress, GivenName, TelephoneNumber, and/or URL (for PGP key fingerprints)?

    Andrew - "I'd definitely recommend including some form of contact that *doesn't* depend on the Internet (e.g. telephone). Just in case the security incident is of a kind that stops e-mail being delivered or accessed... And having a reference to PGP fingerprints seems like a good idea, too - one less hurdle in the way when you need to transfer sensitive information in a hurry."
    Peter - SAML Entity and Email system are likely separated. Internet-independent telephone contact not feasible. OpenPGP not as widely used, including x.509 does not seem sensible either.
    Romain - PGP Keys already included elsewhere. Maybe we want to include a free text field for a linkedin account etc
    Heather - email address outside domain or telephone number.
    Scott - interest in keeping bar as low as possible, can generate most buy in with simple email address
    Tom - Requirement for email address but keep recommendation open
    Scott - what will be consumed easily? I.e. PGP - would need to test shibboleth etc
    Romain - unlikely that PGP keys in metadata would be trusted, there are existing databases

    Require email, allow additional telephone number or email addresses if desired. No PGP since it would be duplication. Currently no strong call for a freetext field extension for linkedin etc.
    The email recipient could be anyone/group who would be able to provide security incident response on behalf of the entity. Can leverage local models e.g. SURFConext, where available.

    Correspondence with this address should not be publicly archived.

Action: update training material & security contactType schema info to reflect these recommendations.

b. May contain contact info for department, institution, or NREN CERT?

David proposing to use centralised SURFcert to bulk approve 100 IdPs. General feeling that using existing security groups (or anyone deemed to provide sufficient response) should be encouraged.

c. How “trusted” is the security contact?

What level of verification is the federation doing to check that this won’t bounce, or check that the person is correct? Periodic verification that an email gets to a security function rather than an individual with a new job. **Should add a recommendation for a vetting process into federation operators pack** People are happy to forward information within organisation. For our requirements we just need one listed person at an organisation.

There are automated tools to test pinging. In the US, regularly scheduled tests for weather warnings, could we advertise a “fire drill” and ask for a response within a certain time. Already exists within TFC Cert (but on a small scale). Would need to check that mails do not get blocked etc as scale grows. Spam probability may not be too bad, would target via a platform rather than an email to 1000 recipients. Unclear how this could be managed within Sirtfi. Info shared this morning at CERN, 500 recipients, only 15 redirections - security contact list is generally quite up-to-date. Suspicion that Federations will not do this, due to time or money, maybe could be led by SP community??

What do we do if people don’t respond? Remove them? Metadata would have to be removed/published by federation operators, so the federation operators would need to be kept in the loop. Some debate about appetite of federations vs SPs to work on this, often “operations does not have funding”.

Action: Tom and Scott to take the discussion offline regarding whether this tests should be driven by SPs or by federation operators.

Action: add recommendation to Federation Operators Training Material for them to implement periodic checks of security contact email.

Action: consider practicalities of testing these contacts. Perhaps a discussion for later :)

d. What are the expectations on response?

Should respond in a “timely manner” - difficult to specify precise timeframe, should be discussed on a case-by-case basis. **Should provide guidance on what to do if someone does not respond**

Action: Add guidance to training material for federation participants, “What to do if someone does not respond”, in FAQs

e. Fall back to “technical contact” if no security contact provided?

   Contact would probably forward security information anyway but not same job. Also, could get shared far beyond desired recipients. General agreement not to copy. **Add guidance to use TLP in initial correspondence** Also add that correspondence to this email address will not be publicly archived.

   Action: Add guidance to use TLP when initiating incident response, add to FAQs

f. Use for only IdP/SP incidents or more general account (identity) management or endpoint security incident?

   I.e. should other issues, e.g. software updates, be sent to this address? On one hand the information will probably be forwarded but, on the other, it may be annoying for the recipient. Incidents affecting the entity in the metadata.

   Action: Add guidance on scope of incidents to FAQs

g. Sufficient value to promote security contact registration across federations?

   This was asked to check the WISE audience. Response was that this is a gap that needs to be filled :) Need to be careful to avoid fallback to Google.

2. Andrew - “Also, it would probably be worth talking to Wilfried (if you haven't already done so) about the experiences with the IRT-object in the RIPE database. I suspect there are quite a few lessons in that process that it would be good not to have to re-learn.”

Stalled deployment, we should talk with them. RIPE information is there and has been populated but there are no specific use cases, no context. We don’t have the same problem here since we have the framework.