Wed 9am SantaBarbara

Scribing Template --Wed., Nov 13, 2013 at 9am -- Santa Barbara Room

TOPIC: Federated Incident Response: next steps

CONVENER: Jim Basney

SCRIBE: Scott Koranda

# of ATTENDEES: 25

MAIN ISSUES DISCUSSED: What should be the next steps?

ACTIVITIES GOING FORWARD / NEXT STEPS:

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org

Not all IdPs would be able to respond and not all SPs need to have a response, but for those that could some type of "tagging" would allow a community to form?

UK flags certain IdPs with an "accountability" tag (Nicole reports). Pushback from IdPs is that can only do that for some accounts (not all).

Nicole also observes that none of the policies have anything like incident response, but do say something like "good practice" but that is not defined or pointed to...

Some assurance frameworks (KANTARA for example LOA3) do include this in the framework. Technology independent. Notice is required for LOA3 at 72 hours.

Next step: explore implementation possibilities for that type of KANTARA requirement.

Question: what is value for putting a tag in metadata?

Answer: helps to explain to the consumers/relying parties on what can expect from an IdP

Note that a privacy URL in the metadata is not easily consumable--consuming does not scale since have to read each one.

Argument is made that incident response should be part of assurance.

Incident response is useful but probably only for higher LOA.

Scope discussion today only for notification of incidents or broaden to all aspects of incident response?

Discussion about LOA. Does incident response only get included with "traditional" LOA 3? What about LOA2 + incident response?

Once get to point of "signaling" in metadata, there want to have just a few possible tags/levels, but the discussion of what leads into the signaling is much larger.

Does putting a notification of a "bad" SAML assertion on some list help? Pointed out that the compromise is about more than an assertion, but having bad assertions signaled helps.

Discussion of parallels to X.509 CRLs.

Detail an assertion ID and a time range? Concern about the assertion because of keeping them around and leaking PII.

Having notification of a time range as a minimum is probably a minimum threshold.

Concern about focusing to specific use cases in order to make progress.

There are standard formats for security incident response reporting, consider leveraging those instead of something new. Have to be careful about information sharing. People that care about privacy care and some would react strongly.

Discussion about whether or not the IdP technology plays a role. This in response to question about where we are in the development cycle for Shibboleth IdP v3.

Would the "SAML CRL" be public? Are there privacy issues/implications with a SAML CRL? There is an existing relationship between the relying parties, yes, but argument that need to be careful about giving people "that much rope". Have to explain to relying parties about what they would have in that case.

REN-ISAC has interesting tools. NATO also has some tools and frameworks? Lot of concern over information flow and that gets one control over privacy in the end. **Incident Object Description Exchange Format** (**IODEF**) community has experience with building these types of tools.

Gap to bridge between this community and other communities that have dealt with incident response.

Is notification the right level of "rebundling" for assurance levels, or are there more? SPs make trust decisions in a number of ways. How do we stand up IODEF (?) for federations?

If only one LIGO user on a campus and the campus tells the LIGO SP that there has been an incident that is a PII leak if the disclosure is public.

So want to advertise in metadata what type of incident response an IdP does and SP can decide and can let users know that if there is a response there might be types of incident response that discloses information.

Long discussion on how to operationalize the notification.

Not all trust decisions need to be fully automated. Not all processes have to be automated? "Anything you cannot automate might as well not exist". Debate.

Nicole agrees to help spin up a place in REFEDs to continue this discussion.

How many people involve SIRTs in federated incident response? Have to ask the "security" guys.

MNE-7 was a "GEANT thing" for NATO involved aerospace and so on. Identified need for incident response management for, among other things, cyberwar.

MACCSA look at federatedbusiness.org

Consider older "forensic dropbox".