2020-July-28 CTAB BEv2 Office Hours

Baseline Expectations v2 Office Hours Call, Tuesday, July 28, 2020

Attending

CTAB Members

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska
- Tom Barton, University Chicago and Internet2, ex-officio
- Eric Goodman, UCOP - TAC Representative to CTAB
- Albert Wu, Internet2

Additional Community Members

- Charise Arrowood, Unicon
- Scott Cantor, the Ohio State University
- Gabor Gabanyi, Rutgers
- Meshna Koren, Elsevier
- Les LaCroix, Carleton
- Kyle Lewis, National Institutes of Allergy and Infectious Diseases (NIAID)
- Andrew Morgan, Oregon State University
- Dan Schwartz, Lehigh University

Blog announcing this Office Hour session

For Reference

Community Consensus for Baseline Expectations 2

Previous Baseline Expectations v2 Office Hours

- June 30, 2020 (focus on endpoint encryption)
- May 5, 2020

Discussion

Welcome to the Baseline Expectations v2 Office Hours

ERROR URL

Scott C:

- What is the expectation for BE v2 around ERROR URL?
- Understanding that there will NOT be a requirement to follow the REFEDs specs/guidelines, which were just recently adopted.

Response:

- The proposed BE v2 is that there must be an Error URL.
    - **Proposed BEv2 STATEMENT: All IdP metadata must include an errorURL; if the condition is appropriate, SPs should use the IdP-supplied errorURL to direct the user to proper support.**
- The BEv2 best practice guidelines document will call attention to the REFEDs specs/guidelines and invite organizations to implement it if possible.

Comments:

- Original idea of error URL work was to address insufficient attributes scenarios.
- It will be very helpful to point at the REFEDs specs/guidelines .
- Perhaps over time, some of the material in the REFEDs specs/guidelines could become part of a future version Baseline Expectations

SIRTFI

- **Proposed BEv2 STATEMENT: All entities (IdP and SP) meet the requirements of the Sirtfi v1.0 trust framework when handling security incidents involving federation participants.**
  - **The Sirtfi trust framework v1.0 enables standardized and timely security incident response coordination among federation participants. When signaling and responding to security incidents within the federation, entity operators shall adhere to the process defined in the Sirtfi framework.**
- Albert has talked with Internet2 NET+ team about SIRTFI,
- So far for the BEv2, we have focused on certain parts of SIRTFI, specifically incident response and having a security contact. However, SIRTFI has other statements.
- Do we want to address other parts of SIRTFI more clearly?
- Tom B: there are several obligations as part of SIRTFI, they tend to be somewhat general, to be met with the presence of the entity attribute
- Question:
  - What exactly is the BEv2 requirement for SIRTFI?
  - Is it just a subset of SIRTFI? Section 2.2 of SIRTFI?
- Answer:
  - The BEv2 requirement is for all of SIRTFI within the federation context

Perhaps there are better ways to phrase the proposed SIRTFI requirement, especially the qualifier about “within the federation”

Kyle Lewis:

- Governance questions: will there be a need to re-sign the InCommon agreement for the BEv2?

Response:

- No need to sign the InCommon agreement again.
- The InCommon agreement has compliance with Baseline Agreement “baked in”
- https://incommon.org/wp-content/uploads/2019/04/Participation-Agreement-20180312-Rvw-Copy1.pdf See section 6H
- There is a community consensus process: https://www.incommon.org/federation/community-consensus/
- And Community Dispute Resolution process: https://www.incommon.org/federation/dispute-resolution/

Auditing

- Will there be an audit or report around BEv2 compliance?

Response:

- Checks will happen within Federation Manager, where organizations register their metadata.
- Encryption: Checking that connection endpoints are HTTPS and encrypted
  - May also do more proactive scanning of endpoints for TLS level
- ERROR URL: will check for presence of Error URL
- SIRTFI: the checkbox will be used to assert compliance

Question:

- What about SPs that are just for internal use, but that are registered in Federation?

Response:

- We are looking at this, will likely address this in best practice guidance
- Deregistering these “for internal use” SPs may be an option that organizations want to explore

Comments on SIRTFI

- Les: Regarding SIRTFI, Carleton is likely going by the spirit of SIRTFI, but Information Security Officers hold themselves to a very high standard. The language is somewhat squishy and Information Security officers are reluctant to say “we are SIRTFI compliant”
- Albert: would changing SIRTFI compliance to “we support the SIRTFI framework” be helpful?
- Les: not sure
- EricG: same issues existed at University of California, with CISOs reluctant to say “we are SIRTFI compliant”
- This friction could make it hard to get orgs to check the SIRTFI checkbox
- TomB: perhaps outreach to CISOs would help, as part of the BE V2 implementation process
- DavidB:
  - Also got some pushback from his own organization on “what are we committing ourselves to by asserting SIRTFI?”
  - But TomB provided some helpful answers and eventually got CISO approval to check the SIRTFI box
- AndyM
  - At Oregon State U the IAM dept decided to assert SIRTFI.
  - But now thinking about the consequences of asserting SIRTFI and then in some situation failing in compliance.
- TomB
  - SIRTFI does not address compliance, it’s about capability and intention
  - But an organization that has an issue with another organization’s compliance could potentially lodge a complaint with InCommon. That would go through a dispute resolution process.
- Meshna

    - Elsevier might also have a problem with asserting SIRTFI
    - TomB: would be happy to consult with Meshna on this
- Andy: There was discussion on last BEv2 office hours on testing around TLS and endpoint testing. Wondering about direction for that.
- DavidB:
    - Final language for this BE has not yet been agreed to yet.
    - direction is that BEv2 statement around TLS will be generic, asking InCommon participants to assert that they support endpoint encryption for all endpoints,
    - discussion/guidance will ask organizations to be aware of issues
- Albert:
    - Discussions are ongoing around the BEv2 statement on TLS
    - Definition of what is secure enough will change
    - We want to keep the Baseline Expectations statements elastic
    - InCommon is looking into doing scans to help federation participants understand where vulnerabilities are
    - InCommon can only scan items that are visible outside your firewall
    - Likely SSL labs will be used for scanning, but there are some issues around slowness

- Timing for BEv2:
    - Consensus period should wrap up in August
    - Next there will be a formal proposal
    - Then there will be consultation, could be 6-8 weeks
    - Could be a 6-8 months implementation period before BEV2 goes into effect

Summary of what will be needed during BE v2 implementation period:

- For endpoint encryption, most organizations seem to meet this requirement today.
  InCommon will try to help guide organizations that don't comply to understand what is needed
- For ERROR URL, InCommon can help with language for standing up an ERROR URL page
- SIRTFI: We are hearing that conversations with CISO will be key around SIRTFI

Final question to those on the call

- Are there show stoppers to moving forward with the proposed BEv2 statements?
- (none expressed at this point)

Thanks for joining us today.