Operational Security and Incident Response

AARC2 work can be found at AARC2 NA3 Task 3.1 - Operational Security and Incident Response

AARC

Sirtfi is ready for adoption! The list of Sirtfi compliant Federation Participants can be seen on the eduGAIN Technical site by selecting "asserted" in the Sirtfi dropdown: https://technical.edugain.org/entities

Need Incident Response Now?

Ongoing Security Incident or a nasty suspicion?

Follow the Generic security incident response procedure for federations, and remember to also involve your local federation. Read up at https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf and remember that the eduGAIN technical site has all the site contacts.

Although computer security incident response procedures often exist at the national level, they are rarely formally specified for federations and there is no best practice guidance for security incidents involving several federations spreading across multiple administrative domains. Whilst R&E federations and their underlying IdPs have a long-standing operational tradition, and while the organisation operating federations and IdP have developed a computer security incident response capability to deal with both accidental and deliberate violations of system and network security, there are several challenges remaining. One is a 'lack of expressibility': there is no common way to express to service providers and relying parties what level of incident response capability is available, not its maturity level. Secondly, there is not even a standard way defined how to contact the incident response teams within a federation, IdP, or service provider. The meta-data specifications - whilst providing administrative, billing, and helpdesk contact, did not even suggest previously that a security contact would be useful.

This task, specifically by supporting and by working through the global group defining the Security Incident Response Trust Framework for federated Identity (Sirtfi), addresses these key area. Through the works of AARC, in close collaboration with the global community and with REFEDS, there is now a range of accepted practices and standards:

- The Public Sirtfi Homepage
- The Sirtfi Framework document version 1.0
- Training and outreach material

The Sirtfi category is registered according to RFC 6711 with the IANA LoA Profile Registry at http://www.iana.org/assignments/loa-profiles/ with URI https://refeds.org/sirtfi

Security incident response is also an element of the self-assessment process started for the Assurance Profile task (TNA3.1), and an integral part of the GEANT Data Protection Code of Conduct version 2 draft specification. This AARC task also supports the work towards a globally recognised security contact in federation meta-data as part of the Sirtfi v1.0 implementation plan, which is co-supported by the GEANT Project's 'SIRTFI' task (GN4-2-JRA3-T1), where - in collaboration with AARC - additional Sirtfi processes and tooling are developed.

The current state of Sirtfi process implementation, and how it works out in (simulated) security challenges, is periodically probed through the AARC project. The first challenge was conducted in March 2018 (described in AARC2's 'MNA3.3'), and the report and lessons learned are available in the first challenge report.