eduGAIN Security Incident Response Handbook

Preface 1

Chapter 1. Understanding Your Role and Responsibilities 2

Introduction 2

Roles 2

Scope 3

Responsibilities 3

Federation Participants 4

Federation Operators 4

eduGAIN Security Team 4

Chapter 2. Security Incident Response Procedures 5

Federation Participants 5

Federation Operators 6

eduGAIN Security Team 7

Preface

As with products of any REFEDS Working Group, in this instance the SIRTFI Working Group, this document is a community-developed Best Practice Recommendation. However, as with the SIRTFI Trust Framework itself, these Best Practice Recommendations are most effective when all parties it addresses agree to follow it. Organisations such as Federation Operators or eduGAIN may decide to incorporate adoption of these Best Practice Recommendations into their own policies, as many have done with the SIRTFI Trust Framework.

This document is based on previous work conducted in the AARC2 project[1].

Chapter 1. Understanding Your Role and Responsibilities

Introduction

Attacks have become increasingly global and malicious actors often propagate intrusions via user communities that are widely distributed across multiple administrative domains,

[1] https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf

geographical locations and sectors. As we connect our research infrastructures, educational identity services and user communities worldwide, it has become imperative that we respond accordingly in order to ensure sufficient trust and maintain reputation and operations.

This document defines the roles and responsibilities of those taking part in the Security Incident Response process when a Federation Participant suspects a security incident and has reason to believe that Federation Participants outside its origin federation may be affected.

A **Security incident** is a suspected or confirmed violation of an explicit or implied security policy.

This document is aimed at minimising the impact of security incidents in the eduGAIN federated environment. The objective is to ensure that all security incidents are investigated as fully as possible and that Federation Participants promptly report any suspected incident that may pose a risk to other Federation Participants. Security incidents are to be treated as serious matters and their investigation resourced appropriately.

Roles

Federation Operators are the entities operating the federations that are members of eduGAIN, as listed in https://technical.edugain.org/status.

Federation Participants operate the entities that belong to or are accessible via any eduGAIN member federation, including Service Providers, Identity Providers, Attribute Authorities, Research Community AAIs, identity and service provider Proxies, or e-Infrastructures. Federation Participants that are directly published in eduGAIN are listed in https://technical.edugain.org/entities/ (note that this list does not necessarily include entities behind Proxies).

The **eduGAIN Security Team**[2] manages incident response at the inter-federation level providing security coordination between federations.

Scope

The procedures below should be followed when trustworthy operation of the federation is in question. More specifically, this document applies to all suspected federated security incidents unless their extent is known, contained within one federation and cannot affect any other party. In addition to federated identities, threats to federated entities such as Identity Providers, Service Providers and Attribute Authorities are also in scope.

This document defines the role of the eduGAIN Security Team as a central coordinator when multiple administrative domains (within one or spanning multiple federations) are suspected to be affected by an ongoing incident.

Nothing in these procedures is meant to restrict the flow of information among Federation Participants, Federation Operators and external parties. Likewise, nothing in these procedures is meant to supersede established Federation Participant or Federation Operator incident response policies or procedures. They are, however, intended to augment local procedures when an incident may extend beyond the local domain.

[2] https://edugain.org/edugain-security/

Federation Participants that support the Sirtfi framework[3] will receive full Incident Response information and support. Federation Participants that do not support Sirtfi may receive limited information and support.

Responsibilities

Federation Participants, Federation Operators and the eduGAIN Security Team are mutually responsible for diagnosing and resolving the ongoing security incident by ensuring that it is contained, coordinating the response between the affected parties, tracking the progress of the incident response process, disseminating information and providing expertise and guidance.

Federation Operators and the eduGAIN Security Team are expected to marshal concerned Federation Participants and Federation Operators to participate in the response to a security incident.

Federation Participants report in-scope incidents to their Federation Operators, and Federation Operators report in-scope incidents to the eduGAIN Security Team. Centralising incident awareness in this manner improves the chance that other affected parties can be identified and alerted sooner than might otherwise occur, much as a University CSIRT would wish departments within the University to notify them rather than silently resolve just that portion of the incident visible within their department.

Federation Participants

Federation Participants follow the Security Incident Response Procedures for Federation Participants (in Chapter 2 below).

Depending on their expertise and available resources, Federation Participants can also choose to lead the international investigation and coordination of the response to the security incident.

For Federation Participants supporting the Sirtfi framework, the Sirtfi security contact is the channel to engage their incident response team.

Federation Operators

Federation Operators follow the Security Incident Response Procedures for Federation Operators (in Chapter 2 below).

This role is fulfilled by the security contact point identified in their federation profile published in the eduGAIN Member Database. If security contact information is not available then the federation general contacts are used.

In order to fulfil this role adequately, Federation Operators may be supported by Federation Participants, external parties, Research Communities, or e-Infrastructure security teams, as appropriate.

3https://refeds.org/sirtfi

eduGAIN Security Team

The eduGAIN Security Team follows the Security Incident Response Procedures for the eduGAIN Security Team (in Chapter 2 below).

While each Federation Operator and Federation Participant provides security support within their respective domain of responsibility, inter-federation security remains a collective responsibility.

The eduGAIN Security Team supports this responsibility by providing a central contact and support point for security incidents. Its mission is to assist the community by coordinating the investigation and resolution of suspected security incidents that affect Federation Operators and Federation Participants. This includes notifying Federation Participants and Federation Operators or any other relevant party about attacks potentially affecting them.

The expertise and experience accumulated by the eduGAIN community as it defends against attacks is invaluable. The eduGAIN Security Team ensures that lessons learned, statistics and other useful information are disseminated appropriately to improve our security posture as a global, united community.

Chapter 2. Security Incident Response Procedures

The procedures below use the Traffic Light Protocol[4] (TLP) to mark information being shared according to its sensitivity and the audience with whom it may be shared. Specified TLP rules have to be strictly abided during any communication.

If a suspected security incident is discovered to be a false positive, the procedure may be stopped after appropriate notification of the involved parties.

All actions detailed below are understood to be on a best-effort basis and that some parties at times may not be able to do all that is specified by the procedure.

Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort invested in doing so should be commensurate with the scale of the problem and with the potential damage and risks faced by affected parties.

In the event of conflict between this procedure and other applicable policies or procedures for your organisation, local policies and procedures take precedence. If for any reason this procedure cannot be followed, the security contact of the Federation Operator (for Federation Participants) or the eduGAIN Security Team (for Federation Operators) must be notified.

Federation Participants

1. Follow all security incident response procedures established for your organisation and your federation.
2. Initial incident response:

[4] https://www.first.org/tlp/

    a. Contain the security incident to avoid further propagation to other entities, while preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
    b. Report on all suspected ongoing security incidents posing a risk to any Federation Participants within or outside your own federation to your Federation Operator as soon as possible, but within one local working day of becoming aware of the suspected incident.
3. In collaboration with your Federation Operator, ensure that all affected Federation Participants are notified, including those belonging to other federations. Include relevant information, when possible, to allow them to take action.
4. Investigate and coordinate the resolution of suspected security incidents within your domain of operation and keep the Federation Operator and other involved parties updated appropriately.
5. Announce suspension of service (if applicable) to your Federation Operator, in accordance with federation practices.
6. Perform appropriate investigation, system analysis and forensics and strive to understand the cause of the security incident and its full extent.
7. Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear. It is strongly encouraged for such updates to occur at regular intervals, to include the time of the next update within each update and to issue a new update sooner if significant new information is available.
8. Respond to requests for assistance from others involved in the security incident within one local working day (in case of limited trust or doubt regarding the party behind a given request, involve your Federation Operator and the eduGAIN Security Team).
9. Take corrective action, restore legitimate access to service (if applicable).
10. In collaboration with your Federation Operator, produce and share a report, including lessons learned and actions taken, of the incident with all Sirtfi-compliant organisations in all affected federations within one month of its resolution. This report should be labelled TLP AMBER or higher.
11. Review and update your own organisation’s documentation and procedures as necessary to prevent recurrence of the incident in the future.

The Federation Participant's Federation Operator or the eduGAIN Security Team may be contacted and involved at any time for security advice, recommendations, technical support and expertise, regardless of the severity of the suspected incident, at the discretion of and based on the needs of the Federation Participant.

Federation Operators

1. Follow all security incident response procedures established for your federation and for eduGAIN.
2. Report any suspected federated security incident unless its extent is known, contained within one federation and cannot affect any other party to the eduGAIN Security Team, as soon as possible, but within one local working day of becoming aware of the

suspected incident.

3. Assist Federation Participants in performing appropriate investigation, system analysis and forensics and strive to understand the cause of the security incident and its full extent.
4. In collaboration with the eduGAIN Security Team, ensure that all affected Federation Operators and Federation Participants are notified. In addition, if any other federations are affected, ensure the eduGAIN Security Team is notified, even if the affected Federation Operators have been contacted directly.
5. Investigate and coordinate the resolution of suspected security incidents within your domain of operation and keep the eduGAIN Security Team, Federation Participants and other involved parties updated appropriately.
6. Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
7. Assist and advise Federation Participants in taking corrective action, or restoring access to services (if applicable) and legitimate user access.
8. In collaboration with Federation Participants and the eduGAIN Security Team, produce and share a report, including lessons learned and actions taken, of the incident with all Sirtfi-compliant organisations in all affected federations within one month of its resolution. This report should be labelled TLP AMBER or higher.
9. Update your own federation documentation and procedures as necessary to prevent recurrence of the incident in the future.

The eduGAIN Security Team may be contacted and involved at any time for security advice, recommendations, technical support and expertise, regardless of the severity of the suspected incident, at the discretion of and based on the needs of the Federation Operator.

eduGAIN Security Team

1. Act as a central contact and support point for security incidents reported by Federation Operators or Federation Participants.
2. Assist Federation Operators and Federation Participants to identify the cause of security incidents, which may include performing appropriate investigation, system analysis and forensics and strive to understand the cause of the security incident, as well as its full extent.
3. In collaboration with their respective Federation Operators, ensure all affected Federation Participants are notified via their security contact within one local working day.
4. Coordinate the investigation and resolution of suspected security incidents with affected Federation Operators and Federation Participants.
5. Coordinate the communication with third-parties outside of eduGAIN, if relevant.
6. Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
7. Assist and advise Federation Participants and Federation Operators in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
8. Produce and share a report of the incident, including lessons learned and actions taken, with all Sirtfi-compliant organisations in all affected federations within one month of its resolution. This report should be labelled TLP AMBER or higher. Also produce and publish a TLP WHITE version of the report.

9. Update documentation, statistics and procedures as necessary to prevent recurrence of the incident in the future.