Federated Security Incident Response

Deprecated

This page has been deprecated. Please see Incident Handling for current information.

SIRTFI

Note that this page contains general information about federated incident response. See Security Incident Response Trust Framework for Federated Identity (SIRTFI) Category for specific criteria for certification under the SIRTFI program (highly recommended).

Federated identity introduces new challenges for security incident response. Federation participants should consider the impact of federated identity in their incident response practices and treat federated identity partners impacted by a security incident in a similar manner as they would local parties.

Recommended Practice

- Publish federated incident response contact information for your federated services and identity providers.
- Implement a log retention policy for federated services and identity providers.
- Document and advertise your procedure for responding to a federated security incident.

Incident Response Policy

Goal of this Policy

The goal of this policy is to provide a framework for effective security incident response for a federated environment while avoiding conflict with local laws, policies and contractual obligations that participants are bound to outside the scope of this policy. It specifically targets incidents of a security nature and does not attempt to address the complete range of possible incidents in the broad sense of the term. Specifically, the policy aims to:

1. Define what a "security incident" is in the context of federated identity.
2. Define the roles of the parties involved in federated security incident response: user, identity provider and service provider.
3. Define methods to securely determine who one should communicate with at a particular participant regarding a security incident.
4. Provide common expectations for how security incident response occurs.
5. Establish a philosophy of "do for others as you would do for yourself."

The policy is not intended to replace existing local incident response policy. Rather, it is intended to augment local institutional incident response policies and practices, specifically for inter-institutional incidents that require coordination between two or more institutions.

The policy is meant to be applicable to the wide array of institutions that comprise an identity federation such as InCommon, including large, medium and small institutions of higher education as well as digital libraries, government agencies, cyberinfrastucture projects and commercial entities.

Definition of a Security Incident

1. A security incident is the act of violating an explicit or implied security policy (for example, as documented in an acceptable use policy)
2. A Service Provider is expected to define and provide a service. The expected behavior of a service provider is defined by their Participant Operational Practices and possibly other policies and laws. All SPs are expected to comply with any restrictions on the use of attributes contained in the Participant Operating Practices of any Identity Provider partners from which they accept identity information. Evidence of behavior by a service provider that violates those policies is considered a security incident.
3. Identity Providers are expected to represent user identities (identifiers and/or attributes) to the degree of authority and accuracy specified in their Participant Operating Practices. Evidence of failure of an Identity Provider to do so, e.g. impersonation of a user by another party, is considered a security incident.

Reporting a Security Incident

The following procedure assumes Federation participants have published one or more security Contacts in Metadata for the purposes of security incident response.

1. A participant discovering a security incident should strive to notify any affected parties in the federation to the extent allowed by that participant's policies, relevant laws and resource constraints.

2. Participants should maintain a current point of contact for security incident reporting (see "Security Contacts in Metadata" below).
3. Participants, when discovering a security incident, should strive to report the incident to other affected participants at the provided point of contact for security incident response. For example:
    a. If an Identity Provider discovers a security incident that affects one or more Service Providers, it should strive to contact those Service Providers and share relevant information.
    b. If a Service Provider discovers a security incident that affects one or more Identity Providers, it should strive to contact those Identity Providers and share relevant information.
    c. If a security incident involves a user, the incident should be reported to that user's Identity Provider at the provided point of contact for security incident response.
4. Participants should encrypt incident communications to prevent unauthorized disclosure.
5. Service Providers have ultimate authority for access control for their services. A Service Provider may choose to locally de-authorize a user or Identity Provider for any reason, including containment of a security incident.
6. Identity Providers have ultimate authority for access control to their services. An Identity Provider may choose to deny release of user identifiers and attributes to a Service Provider for any reason, including containment of a security incident.
7. A user could be the originator of a security incident report if, for example, they find activity attributed to them at a given Service Provider for which they do not believe they are responsible. The user might report this to either the Service Provider or to their Identity Provider, but in either case, the participant receiving the security incident report should apprise the second participant of the report.

Handling a Security Incident Report

A participant receiving a security incident report ultimately decides what, if any, actions should be taken based on their own resources and relationships with the involved parties. As a goal, a participant receiving a security incident report should strive to treat a security incident report as if it had originated internal to their organization and impacted an internal organizational service, including:

1. Promptly (within one business day) acknowledge receipt of the security incident report.
2. As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible. The participant should follow its own security incident response procedure, treating an incident with a federated service as if the incident had occurred within a local resource or service.
3. Respond to the incident reporter and any other impacted parties when the incident is resolved. The response should provide sufficient information (as allowed by applicable policies and laws) such that any impacted party can determine their own next step(s). For example, if a user's password was compromised, misused to access a Service Provider, and the integrity of that password now restored, that information would allow a Service Provider to re-authorize access by that user.

Sensitivity of Security Incident Information

During the course of an investigation, information about the incident may be shared between participants.

1. Participants should preserve the privacy of all involved and ensure that any confidential or sensitive information is not inappropriately shared.
2. Participants should not share security incident information on behalf of the federation or any other federation member with external parties such as the media without prior agreement. Inquiries regarding security incidents in the federation should be directed to published federation contact points (http://www.incommon.org/contacts).

Auditing and logging

1. Participants are expected to keep internal logs with accurate date/time stamps that allow for security incident response. For example, an Identity Provider should be able to identify the specific individual associated with an anonymised identity presented to a Service Provider.
2. Participants are expected to retain such logs for whatever period of time organizational policy dictates or allows.

Acknowledgements

This material was originally developed by the CIC Identity Management Taskforce (see: CIC Federated Security Incident Response Policy).