Incident Response Procedure

Questions to ask yourself when defining this procedure:

- Where will you store the security contact details of the Infrastructure and its participants?
- How will you maintain up-to-date security contact information?
- Will your infrastructure have a dedicated Computer Security Incident Response (CSIRT) team? If not, how will you source investigative and forensics skills appropriately at short notice during incidents?
- Can your Research Community establish (secure) communication between its participants, management and the wider community?
- Does your Research Community need to set up a secure data store for evidence gathered during Incident Response?
- Do you have established practices to announce suspension of services?

This procedure applies for any suspected or confirmed security breach with a potential impact on the Infrastructure or on other Infrastructure participants.

This procedure is effective from <insert date>.

Security Incident Response Procedure for Infrastructure Participants

1. Aim at containing the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamps.
2. Report the security incident to the Infrastructure Security Contact point within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Security Incident Response Coordinator (identified by the Infrastructure Security Contact):
    a. Collect and strive to identify indicators of compromise (IoCs)
    b. Share incident status reports and IoCs with all affected participants (a “heads-up” and subsequent updates as needed), in the Infrastructure and federation via their security contact (and, if needed, in other federations and with any external trusted entity involved)
4. Announce suspension of service (if applicable) in accordance with Infrastructure, federation and interfederation practices. Public announcements should not contain details other than “Security operations in progress”, unless agreed otherwise with the Infrastructure Security Contact point.

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

5. Perform appropriate investigation, system and network analysis and adequate forensics, and strive to understand the exact cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
6. Share additional status updates and IoCs as often as necessary to keep all affected participants up-to-date with the security incident and enable them to investigate and take action should new information appear.
7. Respond to requests for assistance from other participants involved in the security incident within one working day and investigate new IoCs being shared.
8. Take corrective action, restore access to service (if applicable) and legitimate user access.
9. In collaboration with the Security Incident Response Coordinator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
10. Update documentation and procedures as necessary.

Security Incident Response Procedure for the Infrastructure Security Contact

1. Assist Infrastructure participants in performing appropriate investigation, system and network analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants.
2. Report the security incident to their federation security contact point within one local working day of the initial discovery or notification of the security incident.
3. Coordinate the security incident resolution process and communication with affected participants until the security incident is resolved:
    a. Collect and strive to identify indicators of compromise (IoCs) from all involved entities
    b. Share incident status reports and IoCs with all affected participants (a “heads-up” and subsequent updates as needed), in the Infrastructure and federation via their security contact (and, if needed, in other federations and with any external trusted entity involved). If other federations are affected, the eduGAIN security contact point must be notified, even if affected participants in all other federations have been contacted directly.
4. Ensure suspension of service (if applicable) is announced in accordance with infrastructure, federation and interfederation practices.

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

5. Share additional status updates and IoCs as often as necessary to keep all affected participants up-to-date with the security incident and enable them to investigate and take action should new information appear.
6. Assist and advise participants in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
7. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER [3] or higher.
8. Update documentation and procedures as necessary.

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).