eduGAIN Security Communications Challenge

Introduction

In incident handling proper communication channels are paramount, the function of these should frequently be assessed.

In communication the standard tool is still e-mail, sometimes in combination with a ticket system and/or with extensions, like cryptographic signing, or encrypted communications.

While the e-mail and ticket systems used do not change often, the contact addresses are rather dynamic and need regular verification.

Any support team responsible for the coordination of activities, like incident coordination need to know about he status of the used communication channels.

A way to assess the foundation of the communication channels is to run so called communication challenges, see for example https://wise-community.org/sccc/, or the reaction tests exercised in GEANT TF-CSIRT.

Communication Challenge Toolset

The used toolset is developed by EGI CSIRT and adapted to the more generic situation we have in eduGAIN. It consists of

- a webserver with a edugain.org server certificate.
- unique url generator.
- script to generate the "personalized" challenge message send to the participants.
- evaluation is done based on analysis of web server logs (access times of the unique urls) and the timestamps of the mail send to the participants.
- the anonymized results will be available in graphical format on the webserver.

Input

Recipients list

The security contacts email addresses will be retrieved from the eduGAIN Database using the APIs published on the technical site.

The addresses will be provided in a CSV file with the following format: <Identity Federation Name>,<Email>.

The script that parses the API is available on the GEANT gitlab:

https://gitlab.geant.org/edugain/edugain-contacts/-/blob/master/identity_federations_security_contacts.py

Mail template (participants)

```
Dear {NAME},

you have received this message to verify the security contact data set in
the eduGAIN Database for your Identity Federation.

Please confirm that this contact is still correct by clicking the following
URL and following the instructions:
  https://challenge.edugain.org/{UNIQUE_URL}

No further action is required except for the above.

Sincerely yours, eduGAIN Security Team
```

The content in "{ }" will be automatically filled by the communication challenge tool-set based on the participants csv file.

Make sure to replace "< >" with meaningful input.

Communication challenge process

1. prepare input files (see Needed input)
2. announcement of the challenge by the entity coordinating the activities in the challenged community, ca 1 week before the run (optional)
3. start the challenge, send the messages with the instructions (see mail template).
4. close the challenge 1 week after sending the message, any reply taking more then a week is probably useless in incident response.
5. Send the result graphic (anonymized) to recipients
6. Follow up on non reacting participants, wrong contact addresses mentioned within the challenge related communications, or unexpected effects of different ticket systems eventually used by different participants.

Expected results

- list of valid contact addresses
- list of invalid contact addresses
- reaction times of the participants