ISGC 2024 Security Day

eduGAIN security Table Top Exercise (TTX)

S. Gabriel[1] D. Groep[1] T. Dussa[2] D. Kouřil[3,4]
D. Kelsey[5] M. Kremers[6] D. Vaghetti[7]

[1]Nikhef

[2]DFN CERT

[3]CESNET

[4]Masaryk University

[5]STFC/RAL

[6]Gèant

[7]GARR

March 25 2024

eduGAIN TTX story

- Intro to the TTX, get into groups, assign roles to groups.
- Background, Current Situation.
- Stage-1, Incident begins, report to IdP/SP Proxy
- Stage-2, Incident verified
- Stage-3, Incident spreads
- Stage-4, Investigation starts
- Stage-5, Incident handling
- Stage-6, Incident resolved, close out report

Motivation/Goal

The goal of the exercise:
Raising awareness of the complexity of IR in large/federated environment

Motivation for the TTX
Test IR procedures and policies in eduGAIN and promote/explain the role/utility of eduGAIN CSIRT

Questions to answer
Identify the organisational obstacles in IR, are the available policies complete enough?

Role-play

Why a role-play:

- Handling a simulated real-life incident affecting a complex environment, to get a better understanding of the risks.
- "Cheap" way to test available policies and procedures, are the sufficient, do they "work"?

Enabled learning objectives

- IdP/SP logfile analysis (check for/find a reported Id).
- know SIRTFI v2, and understand to apply it.
- Know how eduGAIN is organised, role of Federations, eduGAIN and eduGAIN CSIRT.
- Name the risks of federated Identity Management.

Roles

Roles, in order of appearance.

- IsP/SP proxy operator (Fed C)
- *Fed C operator*
- IdP A.1 operator
- Fed A operator (needed)
- *User*
- SP B.1 (Cloud compute infra)
- Fed B operator

Some roles have pretty little to do, can/will be covered by the trainers.

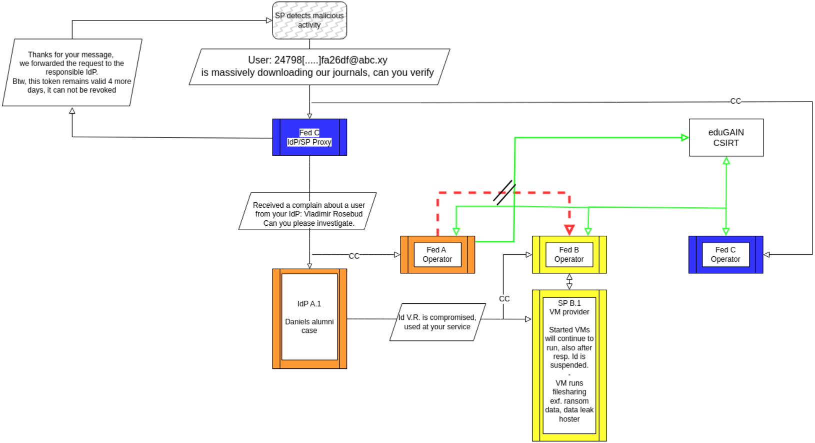
Background, Current situation

Background, Current situation

This game mostly consists of incident elements we handled, though not in the combination we show here.

- We have a couple of IdP, SP and Federation Operators. All participants have carried out a self assessment and announce to be compliant with SIRTI v2. (Hey its a perfect world, isn't it :-))
- Read, discuss your role description, get familiar with your IR tasks.
- if anything goes wrong, rest easy, finding the obstacles is one of the goals of the play.
- if anything is unclear, ask us.

Communications



SP detects malicious activity

User: 24798[.....]fa26df@abc.xy
is massively downloading our journals, can you verify

Thanks for your message,
we forwarded the request to the responsible IdP.
Btw, this token remains valid 4 more days, it can not be revoked

CC

Fed C
IdP/SP Proxy

eduGAIN
CSIRT

Received a complain about a user from your IdP: Vladimir Rosebud
Can you please investigate.

CC

Fed A
Operator

Fed B
Operator

Fed C
Operator

IdP A.1

Daniels alumni case

Id V.R. is compromised, used at your service

CC

SP B.1
VM provider

Started VMs will continue to run, also after resp. Id is suspended.
-
VM runs filesharing exf. ransom data, data leak hoster

What would you do?

During the play you will have to make decisions and report them back to the other players, at each section you should think about what would you do.

When you need information, have instructions for another participants, just raise your hand, we will establish the communication.

Stage-1, Incident begins, report to IdP/SP Proxy