Testing Incident Response Channels and Communications End Points

whilst not overloading the target audience

David Groep
AARC Policy and Best Practice Activity Coordinator
Nikhef

WISE Community meeting, Abingdon
February 27, 2018
Distributed Incident Response and Readiness Challenges

*Sirtfi* version 1 is gaining traction

- provides - self-asserted - security contacts
- point-to-point communications
- interaction not usually visible at the ‘global’ level

we need to now go ‘beyond Sirtfi’

- incidents are not usually bi-lateral
- may spread through federated identity systems
- and outside to relying parties or entire Infrastructure
Beyond Sirtfi: streamlining the response process

trust relationships: allow information to flow rapidly to all that need to know

Infrastructure sharing model: PRACE, XSEDE, ...

Infrastructure sharing model: EGI, WLCG, ...

During Incident Response
Information shared between all participants

Post-Incident-Report Sharing
Information shared between all participants

During Incident Response
Information shared between affected participants

Post-Incident-Report Sharing
Information shared between all participants

graphics: Hannah Short, AARC ‘DNA3.1’ incident response models
Incident response process evolution in federations

Challenges

- IdP appears ‘outside’ the service’s security mandate
- Lack of contact, or lack of trust, in IdP, which is an ‘unknown party’
- IdP fails to inform other affected SPs, for fear of leaking data or reputation
- No established channels of communication

Proposed solutions

- Stronger role for federation operators, as they are known to both SPs and IdPs
- Add hub capability centrally (@ eduGAIN)

graphics: Hannah Short, AARC ‘DNA3.1’ incident response models
Would this model work? You have to test!

Incident Response Test Model for Organisations

*simulated incident to evaluate the model*

- Many participants

- Participants from multiple (existing) infrastructures

- Leverages (and overlaps with) existing groups

Test with these participants was run by Hannah as ‘AARC’ – *phase 1 ran last week*

<table>
<thead>
<tr>
<th>Participant</th>
<th>Role</th>
<th>Federation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERN User</td>
<td>Identity</td>
<td>SWITCHAAI (Full-Mesh)</td>
</tr>
<tr>
<td>INFN User</td>
<td>Identity</td>
<td>IDEM (Full-Mesh)</td>
</tr>
<tr>
<td>Nikhef User</td>
<td>Identity</td>
<td>SurfConext (Hub-and-Spoke)</td>
</tr>
<tr>
<td>LIGO User</td>
<td>Identity</td>
<td>Internet2 (Full-Mesh)</td>
</tr>
<tr>
<td>CERN</td>
<td>IdP</td>
<td>SWITCHAAI (Full-Mesh)</td>
</tr>
<tr>
<td>Nikhef</td>
<td>IdP</td>
<td>SurfConext (Hub-and-Spoke)</td>
</tr>
<tr>
<td>INFN</td>
<td>IdP</td>
<td>IDEM (Full-Mesh)</td>
</tr>
<tr>
<td>LIGO</td>
<td>IdP</td>
<td>Internet2 (Full-Mesh)</td>
</tr>
<tr>
<td>RCAuth Certificate Service</td>
<td>SP</td>
<td>SurfConext (Hub-and-Spoke)</td>
</tr>
<tr>
<td>CERN Marketplace</td>
<td>SP (Behind CERN’s Proxy)</td>
<td>SWITCHAAI (Full-Mesh)</td>
</tr>
<tr>
<td>LIGO</td>
<td>???</td>
<td>Internet2 (Full-Mesh)</td>
</tr>
<tr>
<td>IDEM</td>
<td>Federation Operator</td>
<td></td>
</tr>
<tr>
<td>SurfConext</td>
<td>Federation Operator</td>
<td></td>
</tr>
<tr>
<td>SWITCHAAI</td>
<td>Federation Operator</td>
<td></td>
</tr>
<tr>
<td>eduGAIN Support</td>
<td>Interfederation Operator</td>
<td></td>
</tr>
</tbody>
</table>
Who runs the test?

- Test with these participants was run ‘by AARC’

Logical candidates that could all run the test ... and ‘legitimately’ claim an interest
- eduGAIN
- GEANT.org
- EOSC-HUB ops, or EGI CSIRT
- IGTF
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, OSG, HPCI, ...
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, ...
- any institution (or person) with access to https://mds.edugain.org/

so in a short while, all the email in the world will be on Sirtfi Incident Response tests??
Frequency of challenges and tests - examples

**Trusted Introducer and TF-CSIRT**
- 2-3 Reaction Tests per year
- supported by web click infrastructure, but requires (team) authentication

**SURFcert challenges**
- annual response challenges, just reply to email to a (traceable) ticket

**IGTF RAT Communications Challenges**
- every 1-2 years
- in parallel with continuous operational monitoring

yet we already listed 14 entities that have a real interest in running tests, 5000+ entities can claim the same
How to coordinate – discussion items!

Designate a lead ‘management’ organization for each element? so that each ‘target’ does not get hit by many competing and concurrent challenges?

• e.g. eduGAIN to run communications challenges against Sirtfi email addresses
• the e-Infrastructures to test responsiveness of SPs and RPs with each RP/SP/Site having a primary e-Infra as its home? or can we jointly (EOSC-HUB) run these challenges per continent?
• coordination must be global

Communications challenges also build ‘confidence’ and trust – an important social aspect

• unless you run the test yourself, or get full insight in the results of a challenge, you may not be growing more trust in the entities tested
• so to get that ‘warm and fuzzy feeling of trust’, results (responsiveness measurement data) should be shared but that sharing needs to be confidential as well – limit to WISE SCI checked infrastructures?
Thank you

Any Questions?

davidg@Nikhef.nl