Security Exercises

S. Gabriel

March 26 2024

Motivation

Being a victim of an awareness campaign.

Some general thoughts on security exercises

Context/Reducing the Problem Space

This talk will focus on security exercises addressing:

- Users: Scientists who use IT for their scientific work, **and** Non scientists providing a working environment for the scientists.
- Service providers/operators (admins) providing the tools for the above.
- IT Security professionals,the people that need to deal with situations when things go south.

In an open scientific environment. (Little regulations in place.)

Different Perspectives

Now that we only look at good willing, or at least not willingly disruptive players, what are their goals/priorities? what are their perspectives on the IT security problem?

- Scientists want to solve scientific problems (in our case) using computers. I.e services/tools provided to them for that purpose.
- Service providers (admins) want to make the tools available as efficient as possible.
- Security professionals want to help so that the above 2 can reach their goals.

Which perspective is missing?

Which perspective is missing?

Which perspective is missing?

Which perspective is missing?

- Right, ...the head of the institute/hospital/organization.
- We do research in a certain field, or we are a hospital, we are on this planet to do exactly this, do excellent science/healthcare.
- We risk loose funding if we don't achieve a.b.c. ...
- To achieve a.b.c we need hardware (instruments) and people that can make use of them.

Different Perspectives, focuses, the implied risk perception, and how to handle it.

Risks you say? actually for what or who exactly?

- Scientist: I risk to not finish my research project, paper/presentation etc. if I don't get this "computation" finished in near time. If I use X from unsafe sources, bypass security measure Y, will speed up things.
- Secretary: I need information for the conference I have to organise, this is probably available through this link, if I don't get this in information in time I risk in delaying the planning.
- If I patch now I risk a service availability degradation.
- Security Team: shaking head, if I don't get the above on track soon I risk ending up in a very uncomfortable situation.

How to address the perceived risks, what security exercises have to do with it.

Before running trainings, Prepare for human errors

- Improve resilience (fault tolerance) of the IT infrastructure.
- Allow for efficient incident response in the infrastructure (policies, monitoring, enforcement)
- Identify the weak points, ...human errors, provide specialized training to key personal, basic training for all users.
- Position the security team as the support team that helps to find solutions.

Types of security exercises

Rough categories:

- Technical exercises.
- Procedure checks/ exercises (depend on available security policies)
- Behavioural exercises.

General Requirements on security exercises

- Define a goal, and provide a description how to achieve it.
- Be clear about what to measure and how.
- Define Enabled Learning Objectives (ELOs)

Goals of security exercises, examples

- Measure the insight you have of what is happening in your infra (can you spot incidents).
- Measure/improve resilience of the IT infrastructure so that it can compensate for human errors.
- Measure the incident response efficiency.
  - Put the incident response procedures to a test.
  - Is sufficient forensics expertise available?
- Raise awareness that there are risks, and how to spot them. Avoid making the internet unusable.

How to achieve these goals in our environment

Be transparent with what you do with all participants.

Technical trainings ("easy")

- Plant recorded activities on the infrastructure, measure what can be reconstructed from monitoring
- Red/Blue/Purple team exercises, addressing specific parts of incident handling:
  - Communication channel exercises.
  - Containment (stop/react on malicious processes/accounts).
  - Forensics capabilities.
  - Or shaking the whole tree.

Human behaviour ("complex")

Vulnerability: human psychology

- Role-play, realistic, still artificial play in which security policies and procedure are put to test (see first part of the security workshop yesterday)
- Crisis Management, can be very stressful.
- Awareness trainings, more about that in a minute

Awareness training, or how to safely manoeuvre your security team in a difficult situation

- Make the security team an integral part of the exercise, promote it
- Don't give the participants the impression that they failed a test
- Have solid results (technical)
- Have an idea how to measure the effect over time.