Light weight tabletop exercise

Rain Ottis, PhD

Light weight tabletop exercise

- What is a tabletop exercise
- RED-BLUE

Objectives

- Demonstrate general concepts in cybersecurity, such as:
  - the process of discovering and managing security incidents,
  - common failure points in the security incident management process,
  - the value of cooperation and sharing of information,
  - the limitations of people, processes and technology,
  - the importance of teamwork and clear role assignment,
  - the intersection of information technology, media and law in cybersecurity.

Rules

- Do not fight the scenario
- Stay within the realm of the feasible
- Have fun and improvise
- Players simulate limited knowledge of the situation

Task 1: form teams

- Form teams of 5
  - At least one foreign and one local student
- Pick a team captain
- Team captain sends me a e-mail NLT 21 OCT
  - List the people on the team
  - Brief description of their background
  - Three preferences for team role: Red, law enforcement, ISP, CERT, industry (manufacturing, commerce, etc.), government (ministry, agency)

Instructor feedback 1

- Receive team role assignment and guidance for the exercise preparation

Task 2: onepager

- Send a one page description of your team to the instructor NLT 1200 on 28 OCT 2015, covering the following points
  - role
  - objectives
  - general plan
  - threat assessment

Task 3: Blue team presentation

- On 11 NOV all blue teams will give a short overview of their team, answering questions from all other teams about their:
  - Role, business model, personnel, infrastructure, externally visible security information, etc.
  - If it is conceivable that the BTs/RT would be able to find out, then this information will be given.
  - Instructors decide on borderline cases.

Task 4: Red team presentation

- Closed meeting between RT and instructors to get an overview of Red campaign plan and injects.

Exercise

- 11 NOV - Mock scenarios prepared by instructors
- 25 NOV – Execution of the tabletop, immediate feedback
- 09 DEC – Extended feedback

Inject

- A storyline event
  - Who detects the event?
  - What do they detect?
  - When?
  - Where?
  - Why/how do they detect?
- Discussion – (how) will it reach security staff?

Example inject 1

- Who: intern at MinCOMM
- What: e-mail from MinCOMM IT saying that she should change her account password to “fh49f#D&“ in order to comply with the security policy. Instructions included.
- When: Monday morning at 1000
- Where: MinCOMM
- Why/how: reading daily e-mail

Example inject 2

- Who: PR specialist at ISP
- What: several third party websites hosted by the ISP webhosting service seem to be defaced by L337H4XX0R.
- When: Monday morning at 1000
- Where: ISP HQ
- Why/how: phone call from a news reporter

Example inject 3

- At 1015 on Monday, the News sysadmin gets an automated alarm on his smartphone. It seems the web server has crashed.

Rationale

- What actually happened?
- What was the motivation behind the attacks?

Source

- Ottis, R. (2014). Light Weight Tabletop Exercise for Cybersecurity Education. Journal of Homeland Security and Emergency Management, 11(4), 579 - 592.