Tabletop Exercises

How to Successfully Run Incident Response Tabletop Exercises

Barry Suskind

Senior Director (retired) Threat Detection & Response, Cybersecurity

Intro/agenda

- Who am I and what do I know?
- Agenda

Tabletop Exercises

- What are they?
- How do they compare to disaster/recovery drills?
- What purpose do they serve?

Technical Tabletop Exercises

- Understanding gaps in your enterprise
- Fully exercising cyber security teams
- Having non-cyber technical folks to think more about security
- Learning and putting into practice following procedures
- Teach how to contain information flow

Business Tabletop Exercises

- Engage executive staff in difficult situations
- Understanding the incident response process
- Preparedness for when bad things happen, and they do
- know when to make difficult decisions
- With executives and the board, messaging is key

Combined Tabletop Exercises

- Having both technical, business and executives in one exercise
- Longer meeting times
- Exposes all teams to the complete picture
- Many Challenges

Pre-Planning the Exercise

- What type of exercise?
- How much time should a tabletop exercise take?
- Ensuring incident response plans are current
  - Current list of key personnel and contact information
  - Has technology made aspects of the plan obsolete?
- Scheduling
  - Knowing vacation and operational schedules

Details of an Exercise

- Defining a scenario
  - What aspects of your enterprise will be the target?
  - Understanding the Enterprise and the People
  - Keeping current on industry-wide issues and breaches
- Break the scenario into pieces called “injects”
  - Each inject reveals a bit more information of the “breach”
- Understand timelines
- Don’t skip steps

Sample 1

What is stated in background: security software on a host detected new network activity to an unknown external IP address

What is stated in inject 2: several applications reporting similar activities to multiple external IP addresses

Sample 1

Inject background: after researching open source software used in the enterprise, it is found that use of Apache Ant is prevalent across the enterprise. However, it is found that 15 of the 100 applications using Apache Ant are using a version from 2012 and have never [illegible]

Old and unsupported versions may not [illegible] when vulnerabilities are discovered.

“While not 100% plausible, it shows that keeping up to date with Open Source is important.

Sample 2

background: [illegible] the environment did not have backups, though OneDrive was installed. After after asking questions about the DR and Sharepoint configurations, operations teams could not describe recovery plans

Sample 2

What is stated in inject 1: User contacts helpdesk saying they can no longer open a presentation they were creating. After [illegible] on a [illegible] Macbook

What is stated in inject 2: multiple users contact helpdesk saying they cannot open word documents on their PC’s or they open with gibberish.

Lets Talk About Scenarios

- I’ve created many
- I’ve helped others to make it more plausible
- Frustrations when I was only a participant
- Common take away when 3rd party runs your tabletop
- Consider excluding key persons
- Some examples, just from reading the news
- When speaking with staff about how things work, be careful

Session Hijacking

- MitM with encryption difficult
- AitM via phishing
- BitM via browser takeover

AitM: Auth in the middle
BitM browser in the middle

Microsoft 365

- No conditional access
- Assume cloud protects
- Lack of MFA
- Service accounts and syncing

Executive preparedness

- User infection causes email outage
- External party claims to have data provided by a current employee

Linux/CUPS vulnerability

- Unix/Linux printing service
- RCE, but only maybe

Running the tabletop

- Introduction
- The exercise
- Close out
- Next steps

After the tabletop

- Prepare action report
  - Detail the exercise
  - Highlight the gaps
- Create executive summary
  - Make sure this has a positive spin
- Assign corrective actions to appropriate teams
  - Want actions to be done in a timely fashion

Pitfalls Of Tabletop Exercises

- Challenges with using outsourced incident response vendors
- Scheduling
- Disbelievers
- Lack of attendance
- Lack of engagement during exercise
- Difficulties in completing corrective actions

It’s a wrap

- Types of Tabletop Exercises
- Primary Elements of the exercise
- How to run the exercise and handle questions
- Dealing with the results and outcomes
- Working with third parties to facilitate your Tabletop Exercise