TABLETOP EXERCISE RANSOMWARE

Based on CISA Tabletop Exercise Packages

WISEFROG
‘s-Hertogenbosch, The Netherlands
Document date: 08/11/2024

CONTENTS

Exercise overview 2

General Information 3

- Building Resilience 3
- Participant Roles and Responsibilities 3
- Exercise Structure 4
- Exercise Hotwash and Evaluation 4

Module 1 – Handling external threats 5

- Scenario 1 – CISA alert about a ransomware 5
- Scenario 2 – OS end of support life incident 5
- Scenario 3 – Loss of hardware 5
- Scenario 4 – Phishing attack 5
- Discussion Questions 6

Module 2 – successful attack mitigation 8

- Scenario 1 – Increase in outgoing traffic 8
- Scenario 2 – Ransom demand on computers 8
- Scenario 3 – Leakage of Personally identifiable information 8
- Scenario 4 – Media attention on a cyber incident 8
- Discussion Questions 9

Trainers 11

Training location facilities 12

Contact Information 12

Supplier Information 13

About WiseFrog 14

Terms and Conditions 15

EXERCISE OVERVIEW

Exercise Name	Tabletop Cybersecurity Incident Simulation	
Exercise Date, Time, and Location	TBD	
Exercise Activities	**Time**	**Activity**
	30 Minutes	Threat Briefing and Opening Remarks
	90 Minutes	Module 1
	20 Minutes	Break
	90 Minutes	Module 2
	30 Minutes	Hotwash
Purpose	Examine the cyber resilience of the Client in response to a significant cyber incident.	
National Institute of Standards and Technology Cybersecurity Framework	Identify, Protect, Detect, Respond	
Objectives	Examine the response capabilities of Client during a significant cyber incident. Evaluate the ability for Client to coordinate information sharing during a significant cyber incident. Identify areas of improvement in cyber incident response plans and overall organizational resilience during and following a significant cyber incident. Explore Client's plans to recover and restore services, mission critical assets, or systems.	
Threat or Hazard	Ransomware	
Scenario	A threat actor targets Client's system administrator through a phishing email as an entry point into networks/systems. Attackers compromise Personally Identifiable Information (PII) and install ransomware on Client's computers.	
Sponsor		
Participating Organizations	Incident response team	
Points of Contact	Insert Organization POC(s) Contact Information	

GENERAL INFORMATION

Building Resilience

The purpose of the National Cyber Exercise Program's CISA Tabletop Exercise Packages (CTEPs) that will executed by WiseFrog Security are to increase your organization's resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

Participant Roles and Responsibilities

Players have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario.

Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.

Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing
- Scenario modules:
    - **Module 1**: This module introduces several events, including a CISA cyber threat alert release, an operating system that is no longer supported by its developer, a lost laptop, and a phishing email.
    - **Module 2**: This module includes the discovery of significant data exfiltration possibly including PII, and execution of ransomware.
- Hotwash

Structure Note: Modules, timeline dates, and discussion questions included in each module may be modified as desired

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

MODULE 1 – HANDLING EXTERNAL THREATS

Scenario 1 – CISA alert about a ransomware

The Cybersecurity and Infrastructure Security Agency (CISA) issues an Alert regarding a new ransomware variant. This ransomware is being used in a campaign targeting state, local, tribal, and territorial governments, as well as private sector firms.

Scenario 2 – OS end of support life incident

It has been one year since the developer of your current operating system announced that they will no longer develop security patches for your operating system. The final security patch was installed last week. This vulnerability was identified in your recently completed annual risk assessment.

Scenario 3 – Loss of hardware

An employee informs their manager that their work laptop was stolen from their car overnight. The laptop contained sensitive organizational information.

Scenario 4 – Phishing attack

Members of your R&D department receive an email that appears to be from the Vice President of R&D. It instructs them to access a PDF containing details about an unpaid bill from a third-party vendor supporting your organization. Several employees call the Vice President to verify the email's authenticity. She replies that she did not send it, and that there is no outstanding vendor bill. Nevertheless, some employees still open the PDF.

Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired.

1. What are the greatest cyber threats to your organization?
2. What information technology (IT) systems or processes are the most critical to your organization?
3. What cybersecurity threat information does your organization receive?
    a. What cyber threat information is most useful?
    b. How is information disseminated across your organization and by whom?
    c. What actions would your organization take following an alert like the one presented in the scenario?
4. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
    a. What information technology (IT) systems or processes are the most critical to your organization?
    b. Describe your organization's asset management plan and how you prioritize critical assets.
    c. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
5. Does your organization have backups of vital records stored in a location separate from your primary working files/copies?
    a. How frequently do you run backups?
    b. How long do you keep copies of archived files backed up?
    c. How long would it take to restore primary files from backups?
6. Discuss your risk management strategy.
    a. How is it developed/maintained?
    b. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
    c. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
7. Describe your organization's cybersecurity training program for employees.
    a. How often are employees required to complete this training?
    b. Is training required during employee onboarding before granting system/network access?
    c. What additional training is required for employees who have system administrator-level privileges?
    d. What type of training methods or approaches have you found most beneficial?
8. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
    a. What actions does the IT department take when suspicious emails are reported?
    b. What feedback do employees receive after reporting a suspicious email or event?

MODULE 2 – SUCCESSFUL ATTACK MITIGATION

Scenario 1 – Increase in outgoing traffic

An increase in Domain Name System (DNS) traffic outside of standard business hours is flagged by your organization's intrusion detection system and an alert is sent to your IT team/Security Operations Center. Upon further investigation of the system logs, they discover that a significant amount of data was sent from known HR employee IP addresses to external IP addresses.

Scenario 2 – Ransom demand on computers

Computers throughout your organization display a blank red screen. A ransom message then appears demanding €53,000.00 worth of Bitcoin for the decryption key and a warning that the key will expire unless payment is received within 48 hours.

Scenario 3 – Leakage of Personally identifiable information

A security researcher uncovers a series of posts from a well-known hacker group on the Dark Web and contacts your organization. The researcher believes that the posts are genuine, and the threat actors gained access to Personally identifiable information (PII), including <employee social security numbers, bank account and routing number information, etc.>. The hacker group shared a limited number of data records to substantiate their claims and assert their intention to sell the data.

Scenario 4 – Media attention on a cyber incident

News outlets report on the cyber incident. Several news outlets contact your organization for comments on the ransomware infection and data breach.

Discussion Questions

1. Discuss your organization's cyber resilience planning.
    a. What information technology (IT) infrastructure has been identified to support mission essential functions in continuity of operations and incident response plans?
    b. How has your organization prioritized IT infrastructure for restoration?
    c. How has cybersecurity been integrated into your continuity plans?
2. How does your organization baseline network activity?
    a. How can you distinguish between normal and abnormal traffic?
3. Utilizing your organization's cyber incident response plan (CIRP), describe the actions that your organization would take at this time.
    a. Describe the training your employees receive on this plan.
    b. What guidance does the plan include on assessing the severity of the incident?
    c. How does incident severity level dictate response?
    d. How are critical systems and processes incorporated within your CIRP?
4. What redundant systems exist for when primary systems are compromised?
    a. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    b. Who can authorize use of alternate systems or procedures?
    c. How long can you perform manual or alternate processes on your critical systems?
5. What security breach notification laws does your state or industry have?
6. Explain your organization's decision-making process regarding ransomware payment.
    a. Are ransomware policies/procedures included in your CIRP?
    b. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
    c. Discuss the advantages and disadvantages of either agreeing or refusing to pay.
    d. Describe the impact the sale or release of sensitive information or PII would have on your response and recovery activities.
    e. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
7. What capabilities and resources are required for responding to this scenario?
    a. What additional resources outside of your organization would be necessary for responding to the cyber incident?
    b. What are the processes or procedures for requesting additional resources?
    c. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?

8. Describe your organizational processes to respond to the media reports and inquiries.
    a. What pre-scripted messages have been developed for cyber incidents?
    b. What training do your communications personnel receive on cyber terminology?
    c. How would public messaging be coordinated and disseminated during a cyber incident?
    d. How would you preserve and reinforce the public's confidence and trust in your organization during a significant cyber incident?
9. Based on discussion, what changes would you implement to increase the resilience of your organization?

TRAINERS

Nariman Aga-Tagiyev is an Application Security Architect with more than 20 year experience in software development. Have been working as full stack web application developer, backend developer, DevOps engineer, cloud developer and since 2016 fully involved in Application Security related activities.

https://www.linkedin.com/in/aganariman/

Serhat Altın has a strong focus on security by design and secure configuration by default. He excels at creating user experiences that prioritize security without compromising usability, ensuring that systems are both intuitive and inherently secure from the outset. With his deep understanding of secure design principles, Serhat integrates security best practices into every stage of product development, making it easier for users to adopt secure configurations effortlessly.

https://www.linkedin.com/in/serhataltin/

TRAINING LOCATION FACILITIES

The Table Top Exercise will take place at a location selected by the hiring company within the European Union. For locations outside the EU, special quotes can be provided upon request. The following facilities are required:

- A projector and power outlet for the trainer
- Adequate space to allow participants to form working groups of 3-4 people for independent hands-on exercises

CONTACT INFORMATION

We would be happy to have a short call with you to discuss your needs and answer your questions. We do not have aggressive marketing strategy and won't spam you if you get in touch with us.

Contact by email: security@wisefrog.nl

Contact by phone or WhatsApp: +31613732993

Schedule a 30 minutes call: https://calendly.com/aganariman/nariman-30-minutes

SUPPLIER INFORMATION

Company name	WiseFrog
Country of establishment	Netherlands
Address	Willemspoort 102, 5223WV, ‘s-Hertogenbosch, Netherlands
Email (Invoices)	Invoice@wisefrog.nl
Email (administrative)	info@wisefrog.nl
EU VAT-ID	NL003278436B94
KVK - Dutch Chamber of Commerce number	78029260
IBAN	NL92 ABNA 0876 9924 91
BANK SWIFT (BIC)	ABNANL2A
Contact person	Nariman Aga-Tagiyev
Contact person email	nariman@wisefrog.nl
Phone:	+31613732993

ABOUT WISEFROG

Our Story

Founded with a passion for innovation and a commitment to excellence, WiseFrog has been at the forefront of the digital landscape for over a decade. What started as a small team of visionaries has grown into a powerhouse of creative minds, dedicated to pushing boundaries and delivering cutting-edge solutions.

Our Approach

At the core of WiseFrog's philosophy lies a commitment to collaboration and innovation. We work closely with our clients, understanding their unique needs and goals, to deliver tailored solutions that drive tangible results. Our team of experts combines creativity with technical expertise, ensuring every project is executed with precision and attention to detail.

Our Mission

At WiseFrog, we bring together the dynamic worlds of creative media production, innovative product development, and robust cybersecurity. Our mission is to transform ideas into secure, impactful realities. Whether you're looking to create compelling content, develop cutting-edge products, or ensure the highest level of digital security, we're here to make it happen.

Our team consists of passionate creatives, product developers, and cybersecurity experts who are dedicated to excellence in every project we undertake. We believe that every story, product, and system deserves a meticulous and innovative approach. That's why we foster a culture of collaboration and ingenuity, ensuring that your vision is brought to life safely and effectively.

TERMS AND CONDITIONS

1. **Confidentiality**

All information shared by clients during the collaboration will be treated as confidential. Our trainers are committed to maintaining the privacy and security of any sensitive information provided. This data will not be disclosed, shared, or distributed to any third party outside of the training, except as required by law.

2. **Offer Validity**

The offer for this workshop is valid for a duration of 30 days from the date of issuance. After this period, the offer may be subject to change or withdrawal.

3. **Payment Terms**

Invoices for the training must be paid within 30 days following the completion of the workshop. Travel costs related to the workshop are not included in the quoted price and will be invoiced separately after the event. Late payments may incur additional charges or penalties as per WiseFrog's billing policy.

4. **Travel Costs**

Travel and accommodation costs incurred by trainers for on-site workshops will be billed separately after the workshop. These costs will be outlined in a detailed invoice sent to the client.

5. **Cancellation Policy**

Cancellations made up to 7 days before the scheduled training date will be eligible for a full refund. Cancellations made within 7 days of the training will not be eligible for a refund. However, substitutions or rescheduling may be allowed with prior notice.

6. **Liability**

While every effort is made to ensure the accuracy and relevance of the information provided during the training, we are not responsible for any consequences resulting from the use or misuse of the information provided. Clients are responsible for applying threat modeling practices in accordance with their own organizational policies and legal requirements.

7. **Intellectual Property**

All training materials, including presentations, handouts, and digital resources, remain the intellectual property of WiseFrog. Clients are not permitted to reproduce, distribute, or share these materials outside their organization without prior written consent.