SOLUTION BRIEF

Bolster Ransomware Response With FortiGuard Ransomware Tabletop Exercises

Executive Summary

Today's organizations are changing rapidly. Whether it be digital transformation or work-from-anywhere adaptations, change is more of a constant than ever. At the same time, ransomware continues to change and remains as pervasive as ever. With regular changes in tactics, techniques, and procedures (TTPs), security teams and the broader organization must stay on alert for reconnaissance-stage tactics and early footholds that could indicate a potential ransomware attack.

FortiGuard Ransomware Tabletop Exercises (TTXs) can help security teams maintain visibility and a strong understanding of how susceptible their organization is to a ransomware attack. Against the backdrop of change, TTXs provide enterprise teams with real-world scenarios to evaluate their understanding of their processes and playbooks and test their communications efficacy. Security leaders gain visibility into quantifiable gaps and actions for fixing them. By understanding the feasibility and effectiveness of their processes, teams can catch the "gothchas" before they're under fire from an actual ransomware attack. Using the exercise outcomes, security leaders can make informed decisions about how to improve their readiness. TTXs are an important part of security hygiene best practices, particularly given the constant change among networks, people, processes, and threat types.

> "Preparing for ransomware with a tabletop exercise can identify potential gaps and ensure the right process is in place to mitigate and recover from a potential attack."[1]

Why the World Needs It

Are we prepared for a ransomware attack?

Regardless of the specific number of ransomware attacks, variants, or Ransomware-as-a-Service (RaaS) groups, the prevalence and potential impact to an organization that this type of malware can have poses ongoing security concerns. Meanwhile, enterprises are dynamic, living entities with employee turnover, shortfalls in security staff resources and skillsets, and many other challenges. From cloud and new business software adoption to digital transformation initiatives to other organizational changes, the constant technology changes make it difficult for security leaders to maintain a static state of security. Nearly half of executives surveyed feel their security has not "kept up with digital transformation."[2]

Ransomware-specific TTXs are one of several readiness tools that help companies identify and validate current working practices, procedures, and policies to detect and respond to a ransomware attack. These discussion-led exercises can engage just the security team or the broader enterprise teams who are typically engaged during an actual ransomware attack. They provide a forum for constructive discussion in each scenario in which operational plans and processes are reviewed among the exercise participants. The outcome is to enable everyone, not just security leaders, to understand where they can make improvements in their plans so that they're prepared should a ransomware attack occur.

What It Does

The Tabletop Exercise (TTX) Process

FortiGuard Ransomware TTXs are conducted by the FortiGuard Incident Response team based on real-world scenarios to which they've responded.

The TTXs consist of discussion-based exercises that test an organization's playbooks, processes, and communications in detecting and responding to ransomware. Using a series of ransomware scenarios based on the real-world experience of the FortiGuard Incident Response team, facilitators test the organization's incident response plan and assist the team in identifying security gaps in their cybersecurity or processes. Running participants verbally through the scenarios, facilitators guide the company's participants to work together with the provided intelligence from investigations to determine a course of action for each. They ask questions about each scenario and encourage discussion and interaction across the team. This more relaxed environment—while using scenarios from actual ransomware incidents—gives participants the opportunity to assess their abilities while they're not under the pressure of responding to a real incident.

The ransomware tabletop exercise goals: Test a team's playbooks, processes, and communications; help identify gaps; and ultimately lead the team to a clear and concise ransomware incident response action plan.

The key objectives of the ransomware exercises are to:

- Identify and validate current working practices, procedures, and policies
- Identify strengths, weaknesses, and gaps
- Build knowledge and relationships among team members
- Foster more effective communication between teams
- Initiate conversation on how to be better prepared for similar challenges

There are no winners or losers at the end of these scenarios. Instead, the goal is to provide helpful first-hand insight for the team into their overall state of readiness when it comes to detecting and responding to ransomware.

By the end of each testing scenario, each stakeholder should have a stronger understanding of what actions should be taken, and by whom. At the end of the TTX, participants receive a final report that includes policy recommendations for a clear and concise ransomware incident response action plan.

What Outcomes It Helps Drive

TTX outcomes and service options

Change is a constant in every organization. Likewise, so is the ransomware landscape. Ransomware TTXs provide an active, engaged way to assess an organization's processes, communications, and plans, and ultimately their ability to detect and respond to a ransomware incident.

At the close of the exercises, TTXs help leaders and their teams answer the questions:

- What worked well?
- How could we improve?
- What changes or updates to plans, policies, and procedures need to be put in place?

The goal is simple: lead the team to the development of, or update to, a clear and concise ransomware incident response action plan.

For a more comprehensive approach to ransomware preparedness, FortiGuard offers the choice of standalone TTXs or the option of a subscription service with a full suite of proactive and incident response services. The FortiGuard Incident Readiness Subscription Service offers security leaders the ability to better prepare, rapidly respond, and take effective actions at every step. The service is a one-year subscription that provides a comprehensive set of services that includes:

- One readiness assessment
- Sixteen initial service points (64 hours) for:
  - Incident response playbook development
  - Incident response playbook testing (tabletop exercises)
- Digital forensics and incident response (with a one-hour service-level objective)

Additional hours may be purchased as needed.

Strengthen Your Security Posture With Tabletop Exercises

Whether ransomware is here to stay or evolves into the next new threat, TTXs provide security leaders with an understanding of the efficacy of their current ransomware incident response. Security leaders gain visibility to quantifiable gaps and get suggested actions for closing those gaps, ultimately leading to the development of a clear and concise ransomware incident response action plan. Regardless of which service option is chosen, the experience and knowledge gained can inform empowered actions that can withstand changes within an enterprise and across the threat landscape.

[1] Chuck Brooks, "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know," Forbes, June 3, 2022.

[2] ThoughtLab, "Cybersecurity Solutions for a Riskier World," Accessed July 29, 2022.

August 12, 2022 1:30 AM
1700208-0-0-EN