SOLUTION BRIEF

FortiGuard Ransomware Playbook Development

Executive Summary

Today's organizations must pivot rapidly to stay ahead of the changing threat landscape. The rise of digital transformation—along with more companies adopting work-from-anywhere (WFA) strategies—requires security teams to introduce new processes and strategies to protect their organizations. Combine these changes with the proliferation of ransomware, and it's critical not to let ransomware response planning take a backseat or become outdated. This can put additional and unnecessary pressure on security teams.

When a ransomware incident occurs, organizations must know what to do, who to call, and what other critical actions to take to minimize damage, protect data, and maintain or return the business to normal operations. To support security teams everywhere, the FortiGuard Ransomware Playbook Development Service helps organizations create new playbooks or update existing ones. These playbooks are designed to provide decision-makers and pertinent staff with the prescriptive steps to take when an incident occurs, as well as who to communicate with both during and after the breach. With a playbook in place, security leaders can take swift, traceable, and defined actions to recover quickly from a ransomware incident, saving the company's resources and reputation. Playbooks are an integral part of security hygiene best practices as networks, people, processes, and the ransomware landscape evolve.

Why Your Organization Needs a Ransomware Playbook

Regardless of the specific number of ransomware attacks, variants, or Ransomware-as-a-Service (RaaS) groups, the prevalence and potential impact of this category of malware is an ongoing concern for enterprises. Organizations are constantly evolving—from adopting new technologies to managing employee turnover—yet ransomware remains a reality.

These ongoing changes that all organizations face mean that playbooks must be regularly refreshed. For example, what if the company changes cyber-insurance providers or creates a new business unit? If these updates aren't reflected in the playbook, then the organization's incident response plan is at best incomplete, or worse, incorrect.

A ransomware playbook is a valuable tool for organizations to follow, as it includes prescriptive steps to take if and when the organization is faced with a ransomware attack. Knowing what to do is critical, and can help security teams reduce the impact of ransomware. A ransomware playbook contains the prescribed actions and decisions the team must make, including the timing to triage, contain, escalate, and recover from ransomware attack, as well as the key stakeholders and other contacts who must be engaged in the response.

"Risk management strategies should include... having an incident response plan in place if you do get breached."[1]

The number one reason (54%) cited by organizations without an incident response plan was a lack of skilled internal resources for developing that plan.[2]

Developing a Ransomware Playbook

In developing or refreshing an organization's ransomware playbook, FortiGuard playbook developers follow the construct of NIST SP 800-61 Rev. 2, which they customize for each organization, and include the following key areas:

- Preparation
- Detection
- Analysis
- Containment and Eradication
- Recovery
- Post-Incident Activity

The playbook work begins with an interactive development session with key stakeholders, which informs the final step-by-step playbook. Playbook developers call upon their professional experience and expert knowledge of ransomware—from the front lines of FortiGuard Incident Response Services —and understand the critical steps necessary at each stage of the containment, remediation, and recovery processes.

A final interactive customized playbook is provided along with associated files and can be easily updated over time by the organization. The ransomware playbook becomes part of an organization's larger ransomware incident response plan.

Additional Service Options

Every enterprise is in constant flux, just like the evolving ransomware landscape. Ransomware playbooks provide prescriptive steps that enable security teams to be empowered and remain focused during a time of crisis and potential chaos, helping drive specific outcomes despite uncertain circumstances. Ransomware playbooks help guide, rather than overwhelm, security teams so that they can prioritize and make impactful decisions that support business operation continuity.

Because playbooks are only as good as their latest refresh, and imparting their knowledge on those responsible for containing and remediating an incident is critical, they should be regularly exercised and updated as part of a more comprehensive approach to ransomware preparedness. To address this, FortiGuard offers the option of a more inclusive incident readiness subscription. The FortiGuard Incident Readiness Subscription Service offers security leaders the ability to prepare better, respond rapidly, 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 through tabletop exercises
- Digital forensics and incident response, with a one-hour service-level objective

Additional hours may be purchased as needed.

Key Playbook Sections

- Preparation
- Detection
- Analysis
- Containment and Eradication
- Recovery
- Post-Incident Activity

Don't let the lack of in-house expert resources delay having a ransomware playbook or incident response plan. It can mean the difference in the extent of damage and business recovery time if ransomware hits.

Conclusion

As ransomware evolves, current and regularly refreshed ransomware playbooks provide security leaders and their teams with the prescriptive steps they need to quickly and effectively address a ransomware incident thanks to thorough planning.

Whether selecting the simple playbook development option or the broader proactive ransomware readiness planning services, the security team's experience and knowledge gained from these services can inform empowered actions that can stand up against evolving organizations and the ever-changing threat landscape.

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

[2] "The 2021 Ransomware Survey Report," Fortinet, November 3, 2021.

October 18, 2022 10:01 AM

1763114-0-0-EN