SOLUTION BRIEF

FortiGuard Incident Response Plan Development

Executive Overview

From nonprofits to large corporations, organizations need to be prepared to face today's threats head on. When an incident occurs, they must know who is responding, how to respond, and what and when to communicate internally and externally. An incident response (IR) plan helps organizations before, during, and after a confirmed or suspected cybersecurity incident. A well-formulated IR plan also lays out the steps and roles on how to respond, who needs to respond, and what to communicate to the organization to avoid a myriad of setbacks on their way to recovery.

Organizations must know ahead of time 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 Incident Response Plan Development Service helps organizations create a new incident response plan or update existing ones. These plans are designed to provide decision-makers and pertinent staff with the steps to take when an incident strikes, as well as who to communicate with during and after the incident. Incident response plans are a foundational part of security hygiene, especially as the threat landscape continues to evolve.

"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]

Why Your Organization Needs an Incident Response Plan

Organizations are continually under attack from the evolving threats, from the latest ransomware variant to the compromise of sensitive data to a global malware outbreak. An IR plan, approved by senior leadership, provides authority to the IR team to take the necessary actions to respond, eradicate, and recover from a threat. More important, it prescribes actions to take post incident to learn from and improve the organizations security posture.

Without a plan in place, the organization will need to rethink the process of responding to an incident every time, which may lead to anything from not engaging the proper team at just the right time to not communicating with a regulatory authority in the appropriate manner and timeframe. The IR plan will guide the organization and allow for a repeatable process for the most-senior responders to those just joining the organization.

Developing an IR Plan

When developing an IR plan, FortiGuard Incident Response Security Consultants follow NIST SP 800-61 Rev. 2 to design the guiding documentation for the organization's response to any type of cyber incident. This custom document will include details on the IR team, IR communications, and details on key areas of the IR life cycle, including:

- Preparation
- Detection
- Analysis
- Containment and eradication
- Recovery
- Post-incident activity

Incident response plan development begins with an information sharing session with key organization stakeholders to understand the existing people, processes, and technology in place. Additional sessions and document sharing will occur to ensure the IR plan aligns with the organization. Incident response security consultants call on their professional experience and expert knowledge of cybersecurity incidents—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 customized IR plan is provided along with associated appendices, which can and should be updated over time by the organization. The IR plan becomes the foundational, actionable document for the organization's response to cybersecurity incidents.

Although no one-size-fits-all IR template exists, the plan should contain the following items:

- A mission statement
- Goals and objectives
- Scope
- Roles and responsibilities
- Communication procedures
- Incident severity levels
- Incident types
- Incident definitions (incident, event, data breach)
- Incident response procedures

Additional Service Options

Every enterprise is in constant flux, just like the evolving threat landscape. Because IR plans and 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 IR 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 plan development
  - Incident response playbook development of a variety of incident types
  - Tabletop Exercises to exercise the IR plan, playbooks, and IR teams
- Digital forensics and IR, with a one-hour service-level objective
- Additional hours may be purchased as needed.

FortiGuard also offers these services as individual SOWs if desired.

Conclusion

A mature IR program includes a well-developed IR plan that is regularly reviewed (bi-annually) and tested (annually at a minimum). These IR plans are the foundation that will lead the organization through any type of an incident and provide responders with the necessary guidance what they can, but also more importantly, what they cannot do.

From small nonprofits to a large corporation, IR plans empower teams to act and stand up against the evolving 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.

FORTINET

www.fortinet.com

July 1, 2023 2:02 PM
2240368-0-0-EN