SOLUTION BRIEF

Ransomware Readiness Assessment

Executive Summary

Today's organizations have to pivot rapidly to meet the needs of the times. Whether digital transformation or pandemic adaptations in the enterprise, change is now more constant than ever. At the same time, ransomware continues to evolve and remains as pervasive as ever. With continual adaptations of tactics, techniques, and procedures (TTPs), security teams and the broader organization must remain alert to reconnaissance-stage tactics to gain early footholds to protect against ransomware.

To help organizations gain greater visibility and understanding of their current risks to a ransomware attack, **FortiGuard Ransomware Readiness Assessments** can help. Against the backdrop of change, assessments show security leaders quantifiable gaps and provide prioritized actions for closing those gaps. Helping guide and prescribe rather than overwhelm, the assessments can help security leaders make informed, prioritized decisions for the protection of their business. Assessments are an important part of security hygiene best practices as the network, people, processes, and ransomware evolve.

"A risk assessment can quickly identify and prioritize cyber vulnerabilities so that you can immediately... protect critical assets... while immediately improving overall operational cybersecurity."[1]

Answer the Question: 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 of this category of malware is an ongoing enterprise concern. Meanwhile, enterprises are dynamic, living entities replete with employee turnover, shortfalls in security staff resources and skillsets, and many other changes and challenges. From cloud and new business software adoption to digital transformation initiatives to mergers, acquisitions, and 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]

So what can security leaders do to ensure that, regardless of the ongoing enterprise metamorphosis, the enterprise risk level remains low and the business remains viable?

A Ransomware Readiness Assessment is a valuable tool for organizations to understand their ability to withstand a ransomware attack. By providing a regular check-up, ransomware assessments can help security leaders understand any impact—in the form of gaps and impact to risk—that a change to the enterprise may cause. Assessments include prioritized, quantifiable improvements that return the organization to an acceptable risk level, as defined by the business.

The Assessment Process

The Ransomware Readiness Assessment focuses on the implementation and management of incident response cybersecurity practices specific to known ransomware attacks. This includes the TTPs of known ransomware as well as common issues and forensic evidence from across ransomware incidents investigated by the FortiGuard Incident Response team. Each assessment provides guidance on the approach to cybersecurity incident response maturity.

FortiGuard Assessors use the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as the foundation.[3] The framework includes five functional domains that include ~80 maturity practices to assess the state of the organization. These practices are derived from official guidance and the experience of FortiGuard incident responders, who help clients deal with ransomware every week. The incident responders have developed in-depth knowledge of how ransomware gets into an environment, how it spreads, and where clients most often go wrong.

The assessment gauges the organization's overall ability to respond efficiently and effectively to an unexpected ransomware incident. All in less than a week, working around the client's schedule, the process includes a document review followed by focused stakeholder interviews for clarifications and to answer final questions. Assessors establish a baseline, such as the existence of playbooks and incident response planning, identify gaps and the potential impact of those gaps, and then prioritize actions to help mitigate the risk based on the results.

The goal of the Ransomware Readiness Assessment is to strengthen the overall ability of an organization to respond efficiently and effectively to an unexpected ransomware incident and help prioritize cybersecurity actions and investments.

Domain	
Identify	The mix of IT and business-critical assets, threat intelligence, and vulnerabilities that determine an organization's ransomware attack surface
Protect	The defenses in place prevent ransomware vectors or, if an initial compromise is successful, halt further action (lateral movement, credential misuse) by the attacker
Detect	Visibility to ransomware attacker(s) as they enter and scout an environment before they fully strike
Respond	Reactions to ransomware that require a solid game plan with an understanding of the technical options, communication needs, and business impacts
Recover	Clean, protected backups to restore systems quickly and large-scale mitigation planning to minimize a ransomware incident

The final report, the Ransomware Readiness Report, provides maturity scoring through a proprietary tool (allowing easy visualization at a high level) and a set of prioritized, actionable recommendations designed to return the most value for effort and resources. Reports identify specific areas of the incident response processes and procedures to strengthen the overall cybersecurity program, prioritize cybersecurity actions and investments, and maintain the desired level of business continuity and recoverability during an unexpected ransomware incident.

Assessment Outcomes and Service options

Truly, the enterprise is in constant flux—likewise, the ransomware landscape. Ransomware Readiness Assessments provide a current risk understanding in this sea of change. They help guide and prescribe, rather than overwhelm, security decision makers to make prioritized, impactful decisions that can mean the difference in the continuity of their business operations.

For a more comprehensive approach to ransomware preparedness, FortiGuard offers the choice of standalone assessments or the option of a subscription service. 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 (tabletop exercises)
- Digital forensics and incident response (with a one-hour service-level objective)

Additional hours may be purchased as needed.

Conclusion

Whether ransomware is here to stay or evolves to the next threat, assessments provide security leaders with the knowledge and education about their current gaps and the domain-level knowledge of relevant practices to inform their ongoing cybersecurity strategies.

Regardless of which service option is chosen, the experience and knowledge gained can inform empowered actions that can withstand the ebb and flow of the enterprise and the threat landscape.

[1] Chuck Brooks, "A Cybersecurity Risk Management Strategy for the C-Suite," Homeland Security Today, May 11, 2022.

[2] ThoughtLab 2022 Report, "Cybersecurity Solutions for a Riskier World."

[3] NIST Cybersecurity Framework.

August 25, 2022 11:06 PM

1678285-0-0-EN