CHECKLIST

Top Four Steps to Reduce Ransomware Risk

Despite feeling quite prepared for ransomware incidents these days, most organizations have a greater level of concern about ransomware than any other cyberthreat. The experts from FortiGuard Labs, including our threat researchers and incident responders, have outlined fundamental steps to reduce cyber risk.

With ransomware volume exploding 15x over the past 18 months, it's no surprise that 85% of organizations view this as the top cyberthreat facing their organization. Here are the top 4 steps to take to reduce your cyber risk.

☑ 1. Cover the Broad Attack Surface

Today's digital organizations, that increasingly enable work-from-anywhere and utilize cloud services, open up a greater range of possible entry points for ransomware campaigns. The entirety of the attack surface must be identified and security controls distributed across it, including office and home workspaces, corporate and public networks, hybrid and cloud applications, workloads, user and IoT devices, and more.

☑ 2. Deploy Detection and Response Capabilities in Addition to Prevention

In light of sophisticated, multistage ransomware campaigns designed to evade traditional technologies, organizations need to complement strong threat prevention with ongoing inspection for attacks that may have slipped through. This inspection must be applied to all attack vectors and cyber kill chain stages (from reconnaissance through action on objectives), as well as tested and practiced regularly.

☑ 3. Close Gaps and Break Down Silos

While the quality of individual security controls is important to identify cybercampaign components and activity, they must integrate seamlessly in order to share the insight and intelligence necessary to recognize campaigns definitively, rather than just identifying individual aspects that may look ambiguous on their own.

☑ 4. Design for High Scalability

Threat and information volumes are higher than ever, making security a big data problem in many instances. Utilize artificial intelligence (AI) and other advanced analytics to supplement human security experts. But don't overlook the human element—augment teams with outsourced expertise for after-hours coverage or specialized security skill sets and continue to raise security awareness among employees.

Conclusion

According to Gartner, the rapid evolution and sophistication of cyberattacks and the migration of assets to the hybrid multi-cloud create a perfect storm. IT leaders must integrate security tools into a cooperative, consolidated ecosystem using a composable and scalable cybersecurity mesh architecture (CSMA) approach. By 2024, organizations adopting a CSMA to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%.[1] Backing this with well-trained, -skilled, and -practiced employees, staff, and service providers helps organizations greatly reduce their risk of ransomware.

[1] Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, and Patrick Hevesi, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Gartner, October 18, 2021.

www.fortinet.com

February 26, 2022 8:02 AM
1469551-0-0-EN