New FBI Cybersecurity Warning

Richard P. Kusserow | September 2021

Tips to protect against cyberattacks.

The Federal Bureau of Investigation (FBI) issued a cybersecurity alert calling for increased vigilance in network defense practices in response to an increase in ransomware attacks during office closures on weekends and holidays. In 2020 alone, the public reported losses of over $4 billion that resulted from these types of attacks. The number of reported cases increased by about 70% from the previous year.

The FBI encourages all organizations to re-examine their cybersecurity measures and implement its recommended practices to mitigate and manage cyber risks. The alert notes that recent holidays attracted numerous cyberattacks and cites the following as examples:

- Immediately prior to Mother's Day weekend: A critical infrastructure entity in the energy sector experienced a ransomware attack on its information technology (IT) network, resulting in a week-long suspension of operations.
- Memorial Day weekend: The meat production facilities of a critical infrastructure entity experienced a ransomware attack. This resulted in a complete production stoppage.
- Fourth of July weekend: A critical infrastructure entity in the IT sector experienced a ransomware attack that impacted a remote monitoring and management tool and ultimately affected hundreds of organizations.

Health care organizations have proven to be particularly vulnerable to cyberattacks during the COVID-19 pandemic, which has disrupted operations at facilities across the country. For example, the DuPage Medical Group, Illinois' largest independent physician group, recently reported a security breach that affected 600,000 patients.

The FBI alert indicates that the two most prevalent initial access vectors are phishing and brute forcing unsecured remote desktop protocol (RDP) endpoints. Another common method of initial infection is deployment of precursor or dropper malware, which can evaluate a victim's ability to pay a ransom, assess a victim's incentive to pay a ransom to regain access to and/or avoid public exposure of sensitive or proprietary data, and gather information for follow-up attacks.

The FBI's alert further cautions organizations to be vigilant of indications of suspicious activity, such as (a) unusual inbound and outbound network traffic; (b) compromise of administrator privileges; (c) an increase in the permissions on an account; (d) theft of login and password credentials; (e) a substantial increase in database read volume; (f) geographical irregularities in access and login patterns; and (g) attempted user activity during anomalous times.

The FBI suggests engaging in a proactive strategy to prevent attacks or, in the event of a successful attack, minimize damage. Suggested tactics include the following:

1. Establish a baseline of routine IT activity so that any deviations can serve as alerts for action.
2. Review data logs to identify suspicious or anomalous activity.
3. Employ intrusion prevention systems and automated security alerting systems.
4. Appoint IT security employees to be "on call" during times when offices are closed.
5. Provide training on the risks of interacting with malicious websites and opening email attachments.
6. Limit access to resources over internal networks.
7. Filter network traffic to prohibit communications with known malicious IP addresses.
8. Prevent users from accessing known malicious websites by implementing URL blocklists and/or allow lists.
9. Monitor RDP access logs.
10. Enforce account lockouts after a specified number of login attempts.
11. Ensure that devices are properly configured and security features are enabled.
12. Disable ports and protocols that are not being used for a business purpose.
13. Monitor connections between third-party vendors and outside software for suspicious activity.

14. Implement policies that allow systems to execute only known and permitted programs.
15. Require document readers to be opened in protected viewing modes to help prevent active content from running.
16. Upgrade software systems that are no longer supported by vendors to currently supported versions.
17. Regularly patch and update software to the latest available versions.
18. Automatically update antivirus and anti-malware solutions.
19. Conduct regular virus and malware scans.
20. Require strong passwords and challenge responses.
21. Require different passwords for different accounts.
22. Require multi-factor authentication for all services to the extent possible.
23. Implement multiple-layer network segmentation and ensure that critical communications occur in the most secure and reliable layer.
24. Scan the network for open and listening ports and close those that are unnecessary.
25. Secure home networks for employees working remotely.
26. Do not permit the exchange of home and work content.
27. Regularly audit logs to ensure that new accounts belong to legitimate users.
28. Create a cyber incident response plan that includes procedures for providing notifications of ransomware incidents and accounts for the possibility of systems becoming inaccessible.

For more information on this topic, please contact Richard Kusserow at rkusserow@strategicm.com.