RIKER
DANZIG
SCHERER
HYLAND
PERRETTI LLP

New York Department of Financial Services Issues New Guidance on Preventing Ransomware Attacks

Publication:

Cyber Security & Data Privacy Client Alert - July 26, 2021

The ransomware crisis threatens every financial services company and their customers as incidents continue to surge. Many of us have become all too familiar with the term "ransomware" in recent years due to their frequency. Such attacks could severely impact business processes and leave financial organizations without the data they need to operate while undercutting customer confidence.

On June 30, 2021, the New York State Department of Financial Services ("Department" or "DFS") identified cybersecurity controls that significantly reduce the risk of a ransomware attack and should be implemented by companies wherever possible. The guidance was generated from reports to DFS of 74 ransomware attacks from DFS-regulated companies between January 2020 and May 2021. The purpose of these countermeasures is to substantially reduce the risk of a successful ransomware attack and protect every facet of your company. While these controls are well known, it's important to make sure that they are being used. DFS's guidance recommends the following:

1. Train employees in cybersecurity awareness and anti-phishing.

Required cybersecurity awareness training pursuant to 23 NYCRR § 500.14(b) should include recurrent phishing training, including how to spot, avoid, and report phishing attempts.

2. Implement a vulnerability and patch management program.

Companies should have a documented program to identify, assess, track, and remediate vulnerabilities on all enterprise assets within their infrastructure. 23 NYCRR § 500.03(g). The program should include periodic penetration testing. 23 NYCRR § 500.05(b).

3. Use multi-factor authentication, strong passwords and restrict RDP access.
Multi-Factor Authentication ("MFA") protects user accounts and can prevent hackers from obtaining access to the network and from escalating privileges once in the network. All logins to privileged accounts should require MFA, as this is a highly effective way of blocking privilege escalation via password cracking. 23 NYCRR §§ 500.03(d) & (g); 500.12. In addition, companies should ensure that strong, unique passwords are used. 23 NYCRR § 500.03(d). Privileged user accounts should require passwords of at least 16 characters and ban commonly used passwords. Companies should also disable Remote Desktop Protocol ("RDP") access from the internet wherever possible. 23 NYCRR § 500.03(g). However, if deemed necessary, then RDP access should be restricted to only approved (whitelisted) originating sources and require MFA as well as strong passwords.

4. Employ privileged access management to safeguard credentials for privileged accounts.
Companies should implement the principle of least privileged access – each user or service account should be given the minimum level of access necessary to perform the job. 23 NYCRR §§ 500.03(d); 500.07.

5. Use monitoring and response to detect and contain intruders.
Companies must have a way to monitor their systems for intruders and respond to alerts of suspicious activity. 23 NYCRR § 500.03(h).

6. Segregate and test backups to ensure that critical systems can be restored in the face of an attack.
Companies should maintain comprehensive, segregated backups that will allow recovery in the event of a ransomware attack. 23 NYCRR §§ 500.03(e), (f), and (n).

7. Have a ransomware specific incident response plan that is tested by senior leadership.
Companies should have an incident response plan that explicitly addresses ransomware attacks. 23 NYCRR § 500.16. The plan should be tested, and the testing should include decision makers. "Decision makers such as the CEO should not be testing the incident response plan for the first time during a ransomware incident."

As outlined above, such a multi-layered approach to cybersecurity helps to thwart ransomware and other intrusions at each stage of an attack. Regardless, any intrusion by a hacker on a company's internal network should be reported to DFS "as promptly as possible and within 72 hours at the latest," pursuant to 23 NYCRR § 500.17(a). These reports are often the genesis of further investigation by the Department and demonstrating clear and convincing command of the facts helps assure the Department that your company knows how to respond to an incident. A copy of the guidance can be found on the DFS website.

If you have any questions about the new DFS guidance, please contact Michael P. O'Mullan at momullan@riker.com, Labinot Alexander Berlajolli at lberlajolli@riker.com, Robert N. Holup at rholup@riker.com, or any other attorney in Riker Danzig's Cyber Security & Data Privacy practice.

Attorneys:

Michael P. O'Mullan · Labinot Alexander Berlajolli · Robert N. Holup

Practice:

Cyber Security & Data Privacy