Published on *The National Law Review* https://natlawreview.com

Five Strategies to Protect Against Ransomware and Other Cyberattacks

Article By:

Risk Management Magazine

As organizations continue to adapt to remote or hybrid work models, it has never been more vital to have a robust cybersecurity program to better protect against ransomware attacks and other cyberattacks against company systems and personnel. Ransomware attacks have proven a particular risk in recent years, with attacks like the Colonial Pipeline and myriad attacks on health care organizations demonstrating the serious impact of cyberattacks beyond financial risks, affecting everyday life and business operations.

Ransomware and other cyberattacks are always evolving. Attackers are constantly finding new ways to infiltrate environments while trying to stay undetected. Cyberattacks can target many different points in an organization's ecosystem, including firewall configuration, patch management, network segmentation and defensive technology. The following five strategies can help companies mitigate cyberrisk and respond to threats quickly and efficiently:

1. Strengthen Asset Inventory

You cannot protect what you do not know exists or cannot see. Having an efficient asset management program can significantly increase visibility and rapidly provide detailed information about systems in the event of a cyberattack. Organizations should document system or device types, operating systems and software used. To be more granular and aggressive, consider documenting what ports and service systems use for business functions and use that as a baseline for future firewall rules and network exceptions. Having a strong program is key for every organization, but is even more important in remote work environments.

2. Conduct Security Awareness Training

A comprehensive and effective security awareness program for employees benefits the organization at large. An efficient security awareness program extends visibility and cyber threat detection beyond defensive technologies applied in the environment by empowering people to be a critical line of defense. A robust security awareness training program allows employees to assist with the detection of network anomalies, suspicious emails and other potential threats.

3. Assess Antivirus and Endpoint Detection and Response Programs

Traditionally, antivirus programs have helped detect malicious activity. However, the problem with the traditional antivirus approach in modern day cybersecurity is that attackers regularly update their code to obfuscate and bypass signature-based antivirus products. By employing an endpoint detection and response (EDR) product, organizations create an efficient response to detecting malicious programs and activities based on network anomalies rather than signatures alone. If purchasing and implementing an EDR solution is not viable, consider additional layers of defense around the antivirus software. Ultimately, the goal is to increase visibility and the ability to alert upon suspicious activity.

4. Monitor and Detect New Processes

In addition to having inventory on assets, an organization should document legitimate system processes and software. Upon gaining access to an environment, ransomware downloads and executes its installer to infect the victim. Ensuring visibility into your environment can help IT and information security teams to detect programs or processes with behaviors that deviate from the norm. In turn, this allows operations and incident response teams to respond quickly in the event of those anomalies.
One example is Microsoft Windows' AppLocker, which generates messages and alerts about anomalies such as when an attacker attempts to install an executable outside of the known baselined created. By creating baseline rules, AppLocker will create an 8003 warning message that can be collected and parsed using a security incident and event management (SIEM) product or log aggregator and monitored by the IT or information security team.

5. Network Anomaly Detection

Ransomware moves laterally across the network while infecting systems. This can be done quickly while raising flags or network anomalies such as authenticating to several systems within minutes. It is uncommon for systems or domain administrators to connect to multiple systems rapidly and on a large scale on internal networks. To differentiate between legitimate and potentially malicious activity, network administrators must first document legitimate network connections and known behaviors. This supports anomaly detection by establishing outbound and inbound connectivity from the organization's servers. Once the legitimate network connection is documented and a baseline is created, you can leverage defensive technologies and monitoring programs to alert when deviations occur. Then, create alerts in firewalls and SIEM solutions to quickly detect and respond to network anomalies.

As cybercriminals become more advanced, cybersecurity programs must also evolve to identify and prevent malicious behavior. By implementing the best practices and strategies mentioned above, organizations can dramatically reduce their exposure to ransomware and other cyberattacks.

Jonathan Broche contributed to this article

National Law Review, Volumess XII, Number 168

cyberattacks