Ransomware attacks can be extremely destructive to a business and its ability to function. According to a study published in Health Services Research, ransomware adds an extra 2.7 minutes to response times for heart attacks, leading to an additional 36 deaths per 10,000 heart attacks each year. Recovery efforts from ransomware attacks can also damage an organization’s finances and reputation.

Seventy percent of surveyed respondents in the VMware Carbon Black Global Incident Response Threat Report cited they had suffered damage to their corporate image following a breach. Cybercriminals increasingly evolve their attack tools and strategies by developing ransomware variants that slip by legacy malware protection.

Prevention is the most effective defense. By identifying malicious behavior before an attack takes place, these attacks can automatically be blocked.

Follow these 17 best practices recommended by our security experts

1. Implement an awareness and training program. Train users on how to identify and respond to a variety of ransomware attacks, and that it's everyone's responsibility.

2. Block ads. Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads can reduce the risk of malware infections.

3. Inspect east-west traffic (internal traffic). Use traffic analysis to detect threats within your network, and dynamically analyze file behaviors for threats by using AI to detect malicious code.

4. Categorize data based on organizational value. Implement physical and logical separations to protect data and prevent ransomware attacks.

5. Patch operating systems, software and firmware on devices. Ensure that your systems and devices are up to date to mitigate vulnerabilities.

6. Secure your offline backups. Disable backup software that allows unauthorized individuals to restore backups and steal your data.

7. Conduct an annual penetration test and vulnerability assessment. Regular testing helps identify potential weaknesses in your network and allows you to address them before they become serious issues.

8. Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it’s working.

9. Use the principle of least privilege to manage accounts. Users should not be assigned administrative access unless absolutely needed.

10. Use application control on critical systems. Define strict policies for use of applications and scripts on your network to prevent them from accessing your critical assets.

11. Implement physical and logical separation of networks and data for different organizational units.

12. Use a centralized patch-management system. Automate the patch management process to ensure all systems are updated.

13. Establish vulnerability discovery and remediation processes. Once discovered, vulnerabilities must be addressed as quickly as possible to prevent attacks.

14. Configure internal as well as perimeter firewalls. This allows authorized users and workloads to access data, while blocking access to known malicious IP addresses.

15. Logically separate networks. This helps prevent the spread of malware. If every user and server is on the same network, the most recent variants can spread.

16. Use strong spam filters. This is to prevent phishing emails from reaching end users.

17. Log event data. Event logs provide valuable insight into potential security incidents.

Secure your multi-cloud network with the strongest defense against ransomware. Start now by visiting vmware.com/solutions/multi-cloud-security.html

References: