17 Best Practices to Protect Against Ransomware

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. End users are the first line of defense. Educate your users about the threat of ransomware and how to avoid it.
2. Block ads. Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads can reduce that risk.
3. Configure firewalls. This allows authorized users to access data, while blocking access to known malicious IP addresses.
4. 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.
5. Enable strong spam filters. This is to prevent phishing emails from reaching end users.
6. 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.
7. Use the principle of least privilege to manage accounts. Users should not be assigned administrative access unless absolutely needed.
8. Use application control on critical systems. "Default-deny policy for non-approved programs and scripts to stop ransomware before it can access your critical assets."
9. Categorize data based on organizational value. Implement physical and logical separation between data assets of different organizational units.
10. Patch operating systems, software and firmware on devices. Consider using a centralized patch-management system.
11. Inspect east-west traffic (internal traffic). This provides anomaly detection of certificates when encrypted.
12. Inspect north-south traffic. Detect command and control (C&C) traffic by using threat intelligence to identify malicious IP addresses and domains.
13. Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it’s working.
14. Secure your offline backups. Ensure backups are not connected permanently to the computers and networks they are backing up.
15. Conduct an annual penetration test and vulnerability assessment.
16. Use application control on critical systems. Define policy for use of approved programs and scripts to ensure management before it can access your critical assets.
17. Inspect north-south traffic. Detect command and control (C&C) traffic by using threat intelligence to identify malicious IP addresses and domains.

For more information on how you can protect your business with VMware Carbon Black Cloud, visit carbonblack.com/use-cases/ransomware-protection/

References: