WEBROOT®
Smarter Cybersecurity™

10 Fundamentals for Protecting Your Customers from Ransomware

Ransomware attacks are now common, disrupting business operations and costing thousands of dollars in losses. As an MSP, you can protect your business clients from ransomware by understanding the threat and by having the right technologies, policies, people, and processes in place to counter this insidious attack. Here are 10 best practices to consider for protecting yourself and your clients from ransomware.

1

Understand the Threat: Crypto ransomware works by encrypting certain, sensitive files types and then forcing the victim to pay a ransom to gain access to a decryption key for the data. With nearly all types of crypto ransomware it's virtually impossible to recover data without paying for the decryption key. Sometimes even paying the ransom won't decrypt the files.

As an MSP, you need to ensure your infrastructure is adequately secured, and be able to explain to your customers why it's essential they have the technologies and policies in place to protect themselves.

2

Educate Users: It takes one bad decision by a user to unleash a costly ransomware attack. Ransomware is often delivered as a Trojan, through malvertising, or through a phishing email. Prevention isn't possible 100% of the time, but in many cases attacks can still be stopped if users are educated about what to look for.

3

Teach Users Not to Phish: The Webroot® 2016 Threat Brief showed that up to 50% of users will fall for a phishing attack in 2016. The key is to teach users to not open emails from unknown senders with attachments or links – and how to spot suspicious emails even when they look like they're from known senders. Instruct users on spotting expressions or greetings the sender wouldn't normally use as clues to something "phishy." If all else fails, real-time anti-phishing protection can often block even zero-day phishing attacks.

4

Maintain Layers of Anti-Ransomware Technology: Reliable, cloud-based antimalware can prevent nearly all ransomware attacks, but it's important to remember that new delivery vectors are being released constantly, so no endpoint security solution alone will offer you 100% protection. Additional security layers like firewalls, Windows OS policy restrictions, and having proper back-ups in place will all help to secure your environment.

5

Patching and Plug-Ins: Keeping applications like Adobe Reader, Java, and other plugins up to date greatly reduces security vulnerabilities and prevents browser and application vulnerabilities that may bypass your antimalware defenses. Ad and pop-up blockers also greatly reduce user error, stopping users from inadvertently clicking fake dialogs that download ransomware.

WEBROOT®
Smarter Cybersecurity™

6

Use Windows Policies to Block VSS: Blocking access to Volume Shadow Copy Service will help stop ransomware like CryptoLocker from trying to erase file backups. By creating a blocking policy for the VSSAdmin executable, any attempt to access or stop the service will result in the action being blocked.

7

Disable Windows Script Hosting: VBS scripts are used by malware authors either to cause disruption in an environment or to run a process that will download more advanced malware. You can disable them completely by disabling the Windows Script Host engine which is used by .VBS files to run. case of a ransomware attack, they might lose data on every mapped drive.

8

Filter .EXE Files in Email Servers: If your customers' email gateways have the ability to filter files by extension, you should consider denying emails sent with .EXE files, or denying emails sent with files that have two file extensions, the last one being an executable ("*.*.EXE" files). This is a common threat vector for crypto ransomware.

9

Always Have a Back Up: Nothing is more effective at mitigating a crypto ransomware attack than being able to instantly restore data from business continuity backups. As an MSP, you cannot over-emphasize the importance of backups to customers, who sometimes fail to see the value. Remind clients that without a backup they might lose data on every mapped and even unmapped drive. Ransomware such as CryptoLocker can even encrypt networked drives. Having offline air gap or cloud back-ups with multiple copies of each file makes it virtually impossible for extortionists to infect backup data while offering benefits to clients.

10

Stay Current on Ransomware: It pays to keep up with ransomware developments. Some ransomware strains have been cracked, but these are limited successes. Ransomware, like all malware, will continue to evolve. As an MSP, you need to monitor this evolution: which strains are most dangerous and who is being targeted. The more informed you are, the better you can protect customers.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
800 772 9383

Webroot EMEA
6th floor, Block A,
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0)870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900