10 WAYS TO DEFEND AGAINST RANSOMWARE

If there's one attack to be fed up with, it's ransomware. Since COVID, ransomware attacks have skyrocketed and they continue to do so well into 2022. And why shouldn't they? Ransomware has turned so lucrative, entire hacker cartels are being built around it.

Ransomware is also evolving — new methods of attacks are bypassing the traditional spray-and-pray phishing method, and malicious hackers are employing Ransomware as a Service (RaaS) groups to infiltrate an organization in more targeted ways to increase their odds of success. Once infected, these groups can employ double or triple extortion attacks, further compromising victims.

But it doesn't mean companies are defenseless. Even against new types of attacks, companies can employ a variety of security strategies and tactics that can help protect, detect, and respond quickly against ransomware attacks.

HERE'S YOUR LIST OF THE TOP 10 WAYS TO BEAT RANSOMWARE.

01. Have backups (and keep them separate)
Make sure you have backups that are totally disconnected from your network (and ideally, from the internet) so you can recover from a ransomware attack much faster.

02. Keep your employees informed
Employees are still common targets. Teach them how to spot attacks and you'll significantly reduce your risk of falling for a ransomware attack.

03. Secure your accounts
New ransomware attacks take advantage of compromised accounts to ensure a successful attack. Your move? Use 2FA and MFA whenever possible to keep bad actors out of your company's accounts.

04. Cover all your bases
Ransomware attacks can come from anywhere so place a priority on protecting and deploying detection and response tools for email, all endpoints, your Active Directory, and your network.

05. Disable macros
Phishing is still a common way to drop ransomware onto a machine and often hides within macro-loaded excel or Word docs. Disable these from loading by default to minimize your risk.

06. Don't be afraid to limit files, programs, and users
Minimizing what programs, files, and users can do can prevent ransomware from completely infecting your organization. This can be done via Group Policy Object restrictions, whitelisting specific programs, and preventing AD access or changes from unauthorized users.

07. Patch, patch, patch
Attackers can get into an organization and infect a network via exploitable (unpatched) software. Always have your devices and software updated as soon as possible and keep a tight schedule for ongoing updates.

08. Segment your networks
To stop ransomware from reaching your most critical servers and files and doing too much damage, make sure you have some network segmentation in place to isolate those parts of your network.

09. Apply the principle of least privilege
Limit access, especially admin access as much as possible and strip away access from the employees who don't need it. This will reduce the number of accounts that have critical permissions and access to your most sensitive files.

10. Always be monitoring
Speed to reaction is incredibly important against ransomware, so 24x7 monitoring is absolutely needed to ensure immediate detection. You don't want to get hit with ransomware on a Saturday and find out on Monday.

YOU DON'T HAVE TO DO IT BY YOURSELF

These sound like a lot of steps but ransomware is no joke and many of these steps do protect against other kinds of attacks. For companies with fewer resources or who can't make a huge in-house security investment, they should consider an MSSP who can provide guidance, a curated set of technology and tools, and future proofing for your environment to help fight against ransomware.

Consider reaching out to SolCyber. We believe in a minimum dose of security that will protect against ransomware (and much more), and have simplified managed security, ensuring our customers receive best-in-class protection that is faster, simpler and more cost effective to deploy, all in one priced-per-user license.

SolCyber

solcyber.com