FROM THE SOLARWINDS BLOG

How Safe Are Your Backups?

By Nick Cavalancia

Nick Cavalancia is a third-party content contributor and not a SolarWinds employee.

It may seem silly to wonder how safe your backups are; backups are rarely thought of as being at risk. It stems back to a time when backups were on tape—a medium that would be tough for even skilled developers to hack. But today's backups are stored (whether on-premises or in the cloud) on disk or, more specifically, as files in a file system. Depending on how accessible that file system is, your backups may be vulnerable.

In fact, they could be at risk for ransomware. If cybercriminals can encrypt your backup files (along with production data), you'd pretty much have to pay the ransom, no matter how high. Backup files could be important to an attacker in the case of data manipulation or destruction if they're intent on prohibiting you from restoring data to a known good state. In this case, destroying backups could be a strategic move.

Take the following examples of malware and think about how backup data could be accessed:

1. SynoLocker
   This purpose-built ransomware took advantage of a specific vulnerability found on Synology® network-attached storage devices to encrypt the contents.
2. EternalBlue
   This code leverages server message block connections to spread malware across multiple Windows® endpoints.
3. Locky
   This ransomware traversed mapped network shares to find content to encrypt.

While these examples didn't specifically encrypt backup files, the point is that if your backups are accessible to any endpoint (and they likely are), they are at risk.

If you're thinking to yourself, "I'm safe, my backups are encrypted," you're missing the point. Attackers don't typically try to access your backups—they want to *take away your ability to use your backup files*.

KEEPING BACKUPS SAFE

Your mindset should focus on security here. The goal is to protect a dataset that is foundational for protecting other datasets in your organization. Although it isn't an exhaustive list, the following steps are designed to help put your organization in a good position to prevent inappropriate access or manipulation of your backups.

1. Implement least privilege
   To affect your backups, an attacker needs to have access to them in the first place. Try limiting the number of accounts that have access to backup data and restricting the use of those accounts to backup-related processes. In other words, don't use Administrator to perform your backups, as you might log on using those credentials on another system infected with, say, a keylogger.

2. Isolate your backups
   You may want to prevent inbound connections. Set up firewall rules to allow the server performing the backups to operate so that an outbound connection must be established with the system being backed up, while blocking inbound sessions.

3. Maintain multiple copies
   Protecting your backups gives new life to the "3-2-1" backup rule (three copies of your data on two different mediums, with one copy kept off-site). If you're an on-premises backup shop, consider going hybrid cloud or cloud-first instead, as these two flavors of backup were designed to maintain data securely in the cloud. Should on-premises data be manipulated or tampered with in any way, the technique of copying data to the cloud as part of a backup job is intended to help ensure that corrupted data won't be copied off-site.

If you don't take these kinds of proactive steps, your backups could be potentially at risk. Cybercriminal organizations have grown more sophisticated in their tactics and look for ways to ensure their attacks succeed. I think it's natural to conclude that if removing backups from their prey is beneficial to the attacker, they will look for ways to make that happen.

The three steps above are intended to help you reduce the likelihood that your backups will fall victim to an attack.

Nick Cavalancia has over 20 years of enterprise IT experience and is an accomplished executive, consultant, trainer, speaker, and columnist. He has authored, co-authored, and contributed to over a dozen books on Windows, Active Directory®, Exchange™, and other Microsoft® technologies. Nick has also held executive positions at ScriptLogic®, SpectorSoft®, and Netwrix® and now focuses on the evangelism of technology solutions.

Follow Nick on Twitter® at @nickcavalancia

Try cloud-first backup free for 30 days, get the support you need, and pay as you go for only the devices you use.

START YOUR FREE TRIAL

SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses. Learn more today at solarwindsmsp.com