TechTarget Custom Media

A New Approach to Defending your Network Against Ransomware

By David Strom

Defending your network and preventing your users from getting infected with ransomware means more than just implementing various firewalls and network intrusion systems. It is about creating a culture of what Rick Vanover, director of product strategy for Veeam Software, calls being resilient. It is developing a concerted backup and recovery process that will cover your systems and your data assets, so they will be protected when an attack happens and your business can return to an operational state as quickly and as inexpensively as possible. Vanover shared some of his tips for making your systems more resilient.

Backups have traditionally "been a boring part of running a data center," he says. "But that is changing, particularly as storage is cheap and the opportunity cost of lost data is expensive. Your data is valuable and you need to properly protect it." Here are some of his tips on how to become more resilient against fighting ransomware and hardening your backup and recovery processes.

VEEAM

> *"It breaks my heart to see how many enterprises don't test their recovery plans on a regular basis."*

First, understand what you can automate in the recovery process, or what you can automate better. "I heard that one organization, which wasn't using our software, paid the ransom rather than try to recover their data. They calculated that it would be quicker and less expensive with paying the ransom," says Vanover. That shouldn't be the decision. Instead, understand how your backups are needed and how they can be appropriately and best staged to reduce the overall recovery time.

Don't confuse repairing a machine with restoring its data. "The only way to recover your data after an attack is through a restore process. It is never a good idea to repair systems individually," says Vanover. "You can't ensure that the hackers are going to actually deliver a fix as they promise, because after all you are dealing with unknown individuals and there is a risk in working with these kinds of people. Their solution may not be complete, or it may not completely undo your problems and return your lost data." The only sure bet is to use recovery options.

How do you know when you have critical data that isn't being backed up? This is why you need to **test your recovery procedures frequently**. "It breaks my heart to see how many enterprises don't test their recovery plans on a regular basis. Some just do so annually, buy everyone pizza, and accept the number of failures as part of the cost of doing business. That isn't enough, and you have to put forth more effort into regular testing of your data recovery process. I always see an a-ha moment, when my customers finally understand what is important. If they can learn how to perform a recovery quickly, they can save a lot of time when they do have to recover after a breach or an attack. It is really more of an education than a technical problem," he says. Vanover recommends that organizations should test recovery procedures daily, or at least weekly. He mentions that Veeam has an automated recovery verification process that has been part of their product for more than seven years.

Know when your systems are missing backups, or what happens when systems change. Vanover tells the story about one Windows server that had a Registry change but the change didn't take effect until the system was restarted, and then it failed to boot. "If your backups are only good for the last three weeks, and it has been longer since you rebooted that system, you don't have a solid backup to recover from. Under these circumstances, a little problem could become a bigger problem in trying to restore that system."

Part of the problem is that our computing environments are changing constantly.

One of the ways you can test changes to production systems is by using the Veeam Virtual Lab feature. Customers can see what are the implications of any changes in their backup and restoration procedures, and do so in a non-destructive and non-disruptive way that won't take any systems offline while the tests are happening. "We have seen customers use the virtual labs to test various security issues," says Vanover. "Like using a cyber range, to see the impact and risks that happen when a change is implemented. For example, in many circumstances it is difficult to assess whether a SQL server is open to injection attacks, and our virtual lab can illustrate the potential risks.

Part of the problem is that our computing environments are changing constantly. Running servers in the cloud and working on mobile devices, it is easy to see that the volume of data is very dynamic these days. Vanover recommends using a backup vendor that has **regularly scheduled reports that tell network administrators what isn't being backed up**, so that they can take the appropriate corrective action.

Make sure you have everything you need for a complete recovery. Some organizations operate a completely separate disaster computing site, while others employ managed service providers that specialize in this kind of protection that are cloud-based. "A lot of people don't plan the complete disaster recovery experience," says Vanover. "They don't understand what it takes to actually deliver all their applications and servers and data." Sometimes, organizations don't take a complete inventory of all of their digital assets, and only find the gaps when the time comes to recover a lost server that isn't properly backed up. "Even organizations that only have a single data center can suffer from this issue," he says. "They can be dependent on offsite application servers or something outside their data center for their operations. They need to manage their applications appropriately."

"Sometimes I don't want to restore the entire system, just a particular set of data relevant to a single application."

Part of understanding this situation is **matching up the applications and their data needs** and being able to recover exactly what each application needs, especially line-of-business applications. "Sometimes I don't want to restore the entire system, just a particular set of data relevant to a single application. Then I have to ensure that my backups were made appropriately and have the right expectations that my applications are going to be online quickly."

This brings up another point, that organizations **need to have the right amount of Availability with their recovery time objectives**, what Vanover calls "being available enough." This is because the modern enterprise has become more dependent on digital operations, and more dependent on their data being online all the time. The key is having the right kinds of backups that allow for flexible restoration. For example, Veeam offers a specialized recovery feature that allows virtual machines to come back from a backup within a few minutes and be useable.

Becoming more resilient to ransomware isn't a simple process. And, indeed, it is more of a journey than a single destination. Hopefully, these tips can help protect your organization and its operations.