gamechanger Game Changing Technology for Combating Ransomware

What You Need To Know To Prepare Yourself for an Attack

Security providers are working hard to help you protect your organization.

With coverage on TV news and social media of the 2017 global WannaCry attacks, the world knows how extensive and dangerous ransomware has become.

Ransomware attacks represent a serious threat to organizations across a number of industries worldwide. According to the F.B.I., ransomware attacks were on a pace to collect $1 billion in 2016. That figure could go up this year.

The attacks and the organized crime syndicates producing them are getting more and more sophisticated as they search for security holes like unpatched software. Skillful social engineering tactics created by professional malefactors are producing emails designed to appear as if they come from your company's president, or a coworker, personal friend or relative with an attachment that can launch a ransomware attack. It is hard to keep up with these innovations. And even bottom feeders have access to Malware as a Service (MaaS).

But the news isn't all bad. Security providers are working hard developing strategies and technologies to help you protect your organization from these attacks, as well as prepare for recovery in the event you are hit.

PROACTIVE SECURITY

There are proactive actions you can take to help protect your organization before you are infected. If your organization's data does become infected with ransomware, you have recovery options for ways to get your data back. While there may be options outside of paying the ransom, you can expect the authors of the attack will price their own solution to be the easiest and least expensive way to get your data back. If you are not prepared beforehand, you can expect recovery from ransomware to be very expensive.

In the case of ransomware, it is highly recommended you do these four things to protect your organization:

1. Keep all software up-to-date
2. End-user education
3. Least privileged access controls
4. Secure back-up system that includes both local and offsite copies of your organization's data

Like other malware attacks before it, WannaCry took advantage of older systems where security updates and vendor patches had not been applied. If you are not maintaining your firewalls, operating systems and applications, you are leaving the door open to the bad guys.

Other preventive measures include:

- Enable file extensions so users can see what the file type REALLY is
- Make sure Javascript files are opened in Notepad or not opened at all
- Do not enable macros in Office!

Nicescene / Shutterstock.com

End-user education is the simplest protection against ransomware, but often the most difficult to successfully implement. It is not easy to get your end user community to sit down and listen to you tell them why it's a bad idea to open email attachments or download files from the internet. However, a good end-user education program can potentially save your organization millions of dollars if end users recognize the danger posed by email attachments and websites that are not trustworthy. Once-a-year break room PowerPoint lectures are not enough. The best training programs are ones with frequent reminders and testing to keep users on their toes.

Least privileged access is the idea that a user should never have more permission to access your network infrastructure than they absolutely need at that moment. Role Based Access Control, Credential Guard, Remote Credential Guard, Device Guard, Control Flow Guard, Anti-Virus protection, auditing and logging, shielded virtual machines, and containers are all new technologies and features that can be used to ensure a virus does not gain access to administrative rights. It is vitally important that if a user does allow a ransomware virus into your organization's system, that user's access be limited so that the impact of the virus is also limited.

Unfortunately, at least some of you reading this will find that user education and least privileged access are not enough to keep ransomware out of your organization. When you discover that ransomware has encrypted your data, hopefully you'll have the option of recovering from backup. For a backup to be available and effective in restoring your data, you need to put in the time and effort before the attack to ensure your data can be recovered.

For a backup to be available and effective in restoring your data, you need to put in the time and effort before the attack to ensure your data can be recovered.

There are many options for backup services available on the market today. For a backup to be effective it needs to be easy to implement, easy to recover, safe from physical and virtual threats, and most of all it needs to be regularly run against the data that makes your organization work.

You need to understand where your users are saving their data, and you need to understand how to backup that data somewhere safe. In the era of cloud services and BYOD, that job might be bigger than you think.

A good end-user education program can potentially save your organization millions of dollars if end users recognize the danger posed by email attachments and websites that are not trustworthy

3-2-1 BACKUP METHODOLOGY

To prepare for the worst, organizations should assure that they adopt common best practices for data protection including the 3-2-1 methodology. The 3-2-1 principle is have THREE copies of your data on TWO different types of media with ONE copy being offsite.

In addition, performing regular risk assessments should be part of your overall data protection strategy to proactively identify potential risks. As part of the risk assessment, you need to be able to verify that data is recoverable and that it can be restored quickly and easily.

It is also imperative that you safeguard the backup infrastructure by restricting access to the backup repository as well as keeping backup data offline.

However great cloud technology is, it's important not to forget about on-premises based back-up solutions. The recovery speed and security you have by keeping your data on site should not be over looked while you're designing the backup solution for your organization.

Any backup solution needs to be fast, and it needs to be secure. No backup plan can add much protection to your data if it takes forever to complete a single backup job. Nor can it add any value if your data is not secure after the backup is complete. When designing your backup solution ensure that your backup jobs can complete quickly, and your backed-up data is completely secure.

Let's take a look at Veeam's backup and recovery solutions that can help protect your data.

The Veeam Best Practice Solution for Mitigating Ransomware

Be ready to recovery with safe reliable backups.

Ransomware is increasingly sophisticated and consequently difficult to foresee and deal with. While the Veeam solution does not help in preventing ransomware attacks, it can get you prepared and ready to recover from safe, reliable backups, should ransomware hit you.

HOW VEEAM CAN HELP PREPARE FOR RANSOMWARE

Veeam's best backup advice is the 3-2-1 rule for data protection:

- **Three copies of data:** In addition to the primary or production data, there should be a backup copy of the data and a copy of the backup data. Ideally, these would be stored on different physical devices.
- **Two types of media:** It is imperative to use multiple forms of media to prevent ransomware to avoid drives in the same data center from being corrupted. Veeam natively supports backup to a variety of media types including disk, tape, backup appliances and the cloud.
- **One off-site copy:** Veeam's advanced backup and replication capabilities make it easy to have off-site, image-based replication and backup copies to a second location being offsite, tape or the cloud with Veeam Cloud connect. With Veeam Cloud Connect it can store a backup copy off site, to tape or in the cloud. Veeam offers WAN acceleration and encryption to provide fast and secure replications and backup copies.

A secure cloud based backup system will go a long way toward making sure your data can be recovered in the event of a ransomware infection. Cloud based backups can save your organization from an expensive recovery by making sure you don't lose:

- Important files stored on user's laptops
- Server based file shares
- Application data stored in the cloud

Veeam's backup solutions can also create restore points for you on different storage with different retention rules from your standard backup job. Resilient backups are essential to protecting your organization's data in the event of a ransomware infection. Separate restore points on separate media can be invaluable in ensuring that your data can be recovered in the event of a ransomware infection, or several other disaster recovery scenarios.

Finally, included in the Veeam Availability Suite is Veeam ONE, which can be a useful tool to gain visibility into suspicious behavior. It includes predefined alarms that will monitor for unusual write activity with high CPU usage. This pattern can be a good indicator of ransomware. Maintaining Availability for the Always-On Enterprise, Veeam ONE is an integral part of delivering complete visibility and control of your backup and virtual environments. (See Veeam's whitepaper series on ransomware - http://vee.am/ransomwareseriespapers)

A secure cloud based backup system will go a long way toward making sure your data can be recovered in the event of a ransomware infection.

HOW VEEAM CAN HELP RECOVER FROM RANSOMWARE

With a good backup strategy in place, Veeam can help you to painlessly and rapidly recover your data to a known good state through:

- Rapid restores from ransomware attacks through fast VM and granular recovery to override encrypted ransomware databases, applications, files and operating systems.
- Rapid recovery and uninterrupted application performance with tight integration with industry leading storage vendors like Hewlett Packard Enterprise (HPE), Dell EMC, NetApp, Nimble, and soon, IBM.
- Test and discover recovery points to quickly and easily discover last good restore point using Veeam On-Demand Sandbox.

For more information visit www.veeam.com

VEEAM