VEEAM

Mitigating Risk Against Ransomware in the Healthcare Sector

Contents

Introduction

Healthcare institutions hold vast amounts of highly sensitive information on large portions of the population — from basic details such as a person's name and address, to their unique and detailed medical history — and as such, patient records are a high target for ransomware attacks.

Bad actors and cyber criminals seek this data for many different reasons. This valuable data can be used for crimes such as identity theft. Still, healthcare breaches are particularly serious because personal data can, in some cases, mean the difference between life and death. It is, therefore, vitally important for CIOs within the healthcare sector to build secure IT infrastructures that not only withstand ransomware attacks but ensure this critical data remains available.

Ransomware attacks have only intensified under the pressure of the COVID-19 pandemic.[1]

The stakes have never been higher for healthcare to manage, implement, and execute effective data management strategies. Failure to do so will leave them vulnerable to potential ransomware attacks and may have long-lasting implications for their customers' lives and livelihoods.

While the threat of ransomware is an incredibly complex and significant responsibility for organisations — some steps can be taken to mitigate risk from the outset.

In this paper, Rick Vanover, a senior director of product strategy from Veeam, will provide a number of methods to provide the healthcare industry with practical steps to protect data and avoid falling victim to ransomware attacks. These strategies will explore not only how to configure Veeam products to recover from ransomware, but also other tools and techniques to address ransomware head-on.

[1] The rise of ransomware during COVID-19

Education

For the healthcare sector, which holds valuable information on patients, data loss is not an option. As such, the healthcare sector must continue to mitigate risk against ransomware attacks. The first crucial step is by helping detect where ransomware attacks come from, how to identify them, and understanding what IT teams can do to decrease the chances of successful attacks.

Whether it is assessing the phishing risk, removing the most frequent attack vectors, or keeping systems and software up to date, taking these steps is essential for organisations in the healthcare industry to avoid increased risk and attacks.

Education for identifying hacker routes

A malware attack can come from many different sources, however simply knowing that Remote Desktop Protocol (RDP), software updates, and phishing emails are the three main mechanisms for entry is a huge help in focusing the scope of where to invest the most effort to be resilient against ransomware.

- **RDP servers:** It is hard to imagine that in today's IT world, there are still many RDP servers that are directly connected to the internet. The reality is internet-connected RDP needs to stop. IT administrators can get creative with special IP addresses, redirecting RDP ports, complex passwords, and more, but the data does not lie. The fact that over half of ransomware comes in through RDP tells us that exposing RDP to the internet does not align with a forward-thinking ransomware resiliency strategy.
- **Software updates:** While software updates are not a glamourous task, it's a good investment, should another ransomware incident exploit a known and patched vulnerability. Also, keep in mind the need to stay current with updates to critical categories of IT assets: Operating systems, applications, databases, and device firmware.
- **Phishing email**: The other most frequent mode of entry is through phishing email. We've all seen emails that don't make sense or look right. The right thing to do is delete that item, but not every user handles these situations the same way. There are popular tools that can assess the threat risk of phishing success for an organisation. These tools can be useful in measuring an organisation's competency in being able to self-assess the risk of phishing emails, attachments, and more.

Education through preparation:

As part of the preparation process, we also recommend that the organisation becomes familiar with different restore scenarios. This can give the organisation familiarity toward the process, a reasonable expectation of how much time is involved, and most importantly, confidence in that the process will work.

Implementation

Veeam backup products are known for being simple, flexible, and reliable. This is a great set of attributes for organisations within the healthcare sector, looking at strengthening their data management strategy.

When it comes to a ransomware incident, resiliency is based on how an IT team implements the backup solution, the behavior of threat, and the course of remediation. As an important part of ransomware resiliency, implementing Veeam backup infrastructure is a critical step. For IT professionals within the healthcare sector, we've highlighted implementation recommendations below.

Ultra-resilient backup storage and the 3-2-1 Rule

For many years, Veeam has advocated for the 3-2-1 Rule as a general data management strategy. The 3-2-1 Rule recommends that there should be at least three copies of important data, on at least two different types of media, with at least one of these copies being off-site. The wonderful part about the 3-2-1 Rule is that it does not require any particular kind of hardware and is versatile enough to address nearly any failure scenario.

As the threat of ransomware has advanced, Veeam has emphasised that the "one" copy of data be ultra-resilient (i.e., air-gapped, offline, or immutable). Air-gapped or "immutable" backups offer a powerful technique for being resilient against ransomware and other threats by removing the capability of the data being modified, attacked, or deleted. While it can be easily read (using the correct authorisation), malware or intentional attacks cannot change the data. This recommendation is imperative for becoming resilient against ransomware as it provides an impenetrable master of your data to restore from.

Multiple recovery techniques configuration

As with any recovery, getting the data back fast is imperative. By only supporting one type of recovery (for example, VM or Server), you are limiting your recovery options, and possibly elongating the speed of restore. The practical advice in this situation is to have all recovery options available at your disposal and choose the most optimal for the restore need and criticality. The most popular type of restore process usually involves a whole system (i.e., VM or server) recovery, file-level recovery, or application-level recovery.

Endpoint protection

Many organisations know Veeam for data center backups for physical servers, virtual machines, and more. Veeam Agents also provide backup for desktops, laptops, and Windows tablets. Ransomware targets not only servers but also the PCs and devices of your staff. This is ever more important today, with a highly remote workforce storing sensitive data locally.

The strategy for endpoint backups at face value provides an effective ransomware resiliency technique, recovering from backups in the event of an incident. As an added benefit, there is also an opportunity to do continual post-backup scans of endpoint systems, to shorten the time between when a threat comes into a system and the start of an exploit-adding a new layer of protection to your ransomware security posture.

NAS protection

Veeam Backup & Replication's support for NAS backups provides multiple recovery options for file share data if a ransomware incident has compromised the contents. The first type is file and folder recovery for isolated situations that recover based on the last time the backup ran. The second recovery type is to revert the entire share to the specified restore point. The third recovery scenario is to restore the entire share to a new device for a loss-of-device scenario.

Each scenario has a ransomware use case for recovery, but the second scenario provides a compelling way to recover a share to a specific point in time if a ransomware incident has occurred. If, after the attack, part of the NAS share was encrypted or deleted, this restore type can restore the damaged or deleted contents of the share back to the point of time before the attack occurred. For NAS systems that have millions of files and very deep folder paths, the Veeam cache repository will keep track of the file and folder changes within the share. Helping to restore the missing data at the selected point-in-time, without having to know the damage to the contents of the share.

Implementing Veeam capabilities for ransomware detection

Detecting a ransomware threat as early as possible gives IT teams a compelling advantage to quickly limit any potential damage. Veeam has implemented two specific detection techniques to help detect possible ransomware activity.

- **Possible ransomware activity alarm:** This Veeam ONE™ alarm will detect a combination of high CPU activity along with sustained write I/O on a drive. This alarm is customisable as well. The defaults provide a strong baseline reporting for possible ransomware activity and can be fully adjusted to what triggers a specific alarm.
- **Suspicious increment size:** This alarm is a way to report that an incremental backup is suspiciously large. This logic is based on the normal change rate and the possibility that the source data is encrypted, which would remove most storage efficiency opportunities.

Veeam encryption of backup data

In the war against ransomware, it may seem counter-intuitive to recommend encrypting Veeam backup, however, experts recommend encryption for additional resiliency against ransomware and insider threats.

By having the first backup and all subsequent copies of the backup data encrypted, the Veeam backup files are protected against an emerging type of ransomware targeted at data release. There are threat actors that charge a ransom to prevent public data leaks versus to decrypt data. As most organisations would not want a public link to their backup files containing confidential data going out to the highest bidder, then this extra layer of protection is fully warranted. It also defends from insider attacks where malicious employees may try to steal backup data for nefarious activities. Ideally, strong authentication and security would prohibit that from happening, but this is additional protection for peace of mind. Veeam encryption supports a backup job, a backup copy job, a backup to tape job, VeeamZIP, and tape encryption.

Investments in automation

One area that is advisable to have as an additional weapon for ransomware resiliency is in automation. This will specifically help in potential remediation situations, as the original infrastructure may be untrusted due to the attack. There are many Infrastructure-as-Code techniques available with Veeam, Microsoft, VMware, and related technologies that can provision infrastructure, configuration, and key services.

The potential to create an entirely new platform in which to restore via automation is a compelling part of a potential recovery scenario. Consider some of these toolkits as opportunities to rapidly deploy in the event of a need for a complete recovery scenario.

Protection of the Veeam Backup & Replication server and components

While protecting data is the utmost importance, you must protect your backup environment since it has access to your most critical data. Here are some of the most important techniques to consider for implementations:

- **Internet connection:** Keeping the backup server isolated without connectivity to the internet is a fundamental technique to protect against threats getting introduced or propagating.
- **Accounts used for Veeam deployment:** When thinking about which account to use for Veeam deployments, the most resilient approach would be to have as much separation as possible for accounts used.
- **Setting explicit repository access:** For this particular Veeam component, it is recommended that IT professionals prohibit accessing it and browsing it throughout the organisation.
- **Intentionally use Veeam Backup Enterprise Manager:** By using Veeam Backup Enterprise Manager (BEM) for relevant tasks, access to the central control plane of the Veeam infrastructure is significantly reduced.
- **Two-factor authentication:** For the systems that are running Veeam Backup & Replication console roles, it is recommended that you require two-factor authentication to start a remote desktop (RDP) session.
- **Task-specific roles:** Roles provide limits to access as you don't need to provide full admin rights for all backup administrators. These roles can be used with BEM as well as with Veeam Backup & Replication itself. Roles include restore operator, portal user, and portal administrator.

Remediation

Despite all of the education and implementation techniques that are employed to be resilient against ransomware, organisations within the healthcare sector should still prepare for the worst-case scenario.

At Veeam, we recommend the approach to remediating ransomware as:

- **Do not pay the ransom**
- **The only option is to restore data**

With the recommendations previously outlined in this document, organisations should be prepared to have layers of resiliency to defend against a ransomware incident. What organisations may not have thought about is what to do when a threat is discovered. Here are a few recommendations for remediation that should be at your disposal should a ransomware incident happen:

- **Veeam Support:** There is a special group within the Veeam support organisation that has specific operations to guide customers through data restores in ransomware incidents. You do not want to put your backups at risk; they are critical to your ability to recover.
- **Communications first:** In disasters of any type, communication becomes one of the first challenges to overcome. Have a plan for how to communicate to the right individuals out-of-band.
- **Experts:** Have a list of security, incident response, identity management, etc. experts that are ready to be contacted if needed. If a Veeam service provider is used, there are additional value adds to their base offering that can be considered (such as Veeam Cloud Connect Insider Protection).
- **Chain of decision:** One of the hardest parts of recovering from a disaster is decision authority. Who makes the call to restore, to failover, etc.? Have business discussions about this beforehand.
- **Ready to restore:** When the conditions are right to restore, implement additional safety checks before putting systems on the network again.
- **Restore options:** Depending on the situation, maybe a full VM recovery is best. Possibly a file-level recovery makes sense. Familiarity with your recovery options will help greatly.
- **Restore safely:** As explained earlier, Veeam Secure Restore will trigger an antivirus scan of the image before the restore completes. Use the latest antivirus and malware definitions and perhaps an additional tool to ensure a threat is not reintroduced.
- **Force password resets:** Users don't like this but implement a sweeping forced change of passwords. This will reduce the threat propagation surface area.

Conclusion:

Ransomware is no longer a question of *if* but *when*

For organisations in the healthcare sector, the threat of ransomware attacks is real. However, with the right education, technology, and support, organisations can keep both their internal and customer data safe and secure. With the right preparation, the steps outlined in this report can help increase your resiliency against a ransomware incident to avoid data loss, financial loss, incur damage to the business's reputation, and more business reputation damage and more.

You can find more information about Veeam ransomware resiliency resources at:
http://vee.am/ransomwareseriespapers

About Veeam Software

Veeam® is the leader in Backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud, and securing data. With 375,000+ customers worldwide, including 82% of the Fortune 500 and 67% of the Global 2,000, Veeam customer-satisfaction scores are the highest in the industry at 3.5x the average. Veeam's 100-percent channel ecosystem includes global partners, as well as HPE, NetApp, Cisco and Lenovo as exclusive resellers. Veeam has offices in more than 30 countries. To learn more, visit https://www.veeam.com or follow Veeam on Twitter @veeam.

VEEAM

Cloud Data

Backup for what's next

5 Stages of Cloud Data Management — start your journey today!

Learn more: veeam.com