VEEAM

Protecting financial institutions data from ransomware threats

Contents

Introduction

The financial services industry is an attractive target for ransomware attacks. Personal and commercial financial, banking, trading and superannuation information is arguably some of the most valuable data held by an organisation today. The stakes are incredibly high for the financial services industry to adequately protect and secure their systems. Aside from the obvious financial implications of failing to protect data, it can also cause irreparable and immeasurable damage to a company's corporate reputation: shattering trust, eroding customer bases and hindering future sales.

Last year, it was reported[1] that the financial services sector was the second-largest source of data breaches between April-June, with 42 major service breaches taking place in just one quarter.

This has only worsened under the pressure of a global pandemic. In a recent paper on the rise of ransomware under COVID-19[2] by professional services firm KPMG, it was found that remote working significantly increases the risk of a successful ransomware attack. This increase is caused by a combination of weaker controls on home IT networks and a higher likelihood of users clicking on COVID-19-themed ransomware lure emails, owing to heightened levels of anxiety throughout our communities.

The stakes have never been so high for the financial services industry to manage, implement and execute effective data management strategies. Failure to do so will leave organisations vulnerable to potential ransomware attacks, and may have long lasting implications on the business. In many cases, ransomware attackers threaten to publish an organisation's data or perpetually block access to it unless a ransom is paid. However, while the threat of ransomware is incredibly complex and a significant responsibility for organisations, there are steps that can be taken to mitigate risk from the outset.

In this paper, Rick Vanover, a Senior Director in Product Strategy from Veeam, will provide a number of strategies to provide the financial services 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] Financial services sector the second-largest source of data breaches
[2] The rise of ransomware during COVID-19

Education

It is becoming increasingly important for organisations within the financial services sector to mitigate risk against ransomware attacks. The first crucial step is by helping organisations to detect where ransomware attacks come from, how to identify them and understanding what IT teams can do to decrease the chances of attacks breaking through.

Whether it is assessing the phish risk of an organisation, removing the most frequent attack vectors or keeping systems and software up to date, taking these steps are essential for organisations in the industry to avoid attacks. If these steps are not taken, ransomware risk is increased. One way to measure this investment in education is to compare it with the risks, costs and pressure of dealing with a ransomware incident unprepared.

For the financial services sector, which holds valuable information on consumers, data loss is not an option and paying the ransom is not an option.

Education for identifying hackers

From an education perspective, knowing that Remote Desktop Protocol (RDP), phish and software updates 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 on 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.
- **Phish Mail:** The other most frequent mode of entry is through phish mail. We've all seen emails that just 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 phish success for an organisation. These tools can be effective in measuring an organisation's competency in being able to self-assess the risk of phishing emails, attachments and more.
- **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.

Education through preparation:

As part of the preparation process, we also recommend that financial services organisations become 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 that the process will work.

Implementation

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

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

Protection of the Veeam Backup & Replication server and components

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 very important 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 that are 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 main control plane of the Veeam infrastructure is significantly reduced.

An additional technique to reduce the frequency of logging into the Veeam backup server with full permissions is using built-in roles. These roles can be used with BEM as well as with Veeam Backup & Replication itself. Roles include restore operator, portal user and portal administrator.

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.

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 type 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). This recommendation is imperative for becoming resilient against ransomware.

Multiple recovery techniques configuration

In the process of implementing Veeam Backup & Replication, you inherently connect to various other systems. The practical advice in this situation is to have all recovery options available at your disposal. 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. But, Veeam Agents also provide backup for desktops, laptops and Windows tablets. For Linux and Windows backups of endpoints, organisations can add an additional level of ransomware resiliency to the endpoint.

The strategy for endpoint backups at face value provides a ransomware resiliency technique to recover from backups in the event of an incident. There are additional benefits to this as well when the Veeam Data Integration API is considered for endpoint backups. There is also an opportunity to do post-backup scans of endpoint systems to shorten the time between when a threat comes into a system and the start of an exploit.

Veeam Agent *for Microsoft Windows* supports ejecting removable media to make it offline through two critical ransomware resiliency techniques. The first is just having a backup and the second is having a backup be offline. This is supported by Linux systems as well as desktops, laptops and Windows tablets.

NAS protection

Veeam Backup & Replication's support for NAS backups will provide good recovery options for file share data if a ransomware incident has compromised the contents of a file share. The Veeam file backup engine has three types of recovery. The first type is file and folder recovery for isolated situations that recover based on the last time the backup was run. 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 if a ransomware incident has occurred. If the threat is removed but part of the NAS share has been encrypted or deleted, this restore type can take the contents of the share back to what it was at the time of the specified backup. For NAS systems that have millions of files and very deep folder paths, the Veeam cache repository for the share will keep track of the file and folder changes within the share. This is to make a restore to the 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 organisations a compelling advantage and you cannot underestimate the potential of this. 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 are a good starting point for possible ransomware activity, but they can be adjusted to be more conservative in what triggers this particular alarm.
- **Suspicious increment size:** This alarm applies to Veeam ONE when it is monitoring Veeam Backup & Replication in the data protection view. This alarm is a way to report that an incremental backup is suspiciously large. This logic is based on 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 backups. This however is the good type of encryption; It's encryption as a recommendation for additional resiliency against ransomware and insider threats.

The recommendation here is that you use Veeam encryption on backups wherever possible, including in the first backup. The first backup is usually taken on the same site, close to the source data and is generally on an on-premises backup repository. Additional instances of Veeam backup data, such as through a backup copy job or processing onto the Veeam Cloud Tier should also be encrypted.

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. There are threat actors that charge ransom to prevent data leaks versus just to decrypt data. The ransom is taking down data that has leaked out of the organisation. We would not want a public link with some backup files containing confidential data going out to the highest bidder. Ideally, previous recommendations in this document would prohibit that from happening, but this is an additional protection. Veeam encryption is supported for 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. There are many Infrastructure-as-Code techniques available with Veeam, Microsoft, VMware and related technologies.
The various tools in place can provision infrastructure, configuration and key services.

The potential to create a completely new platform in which to restore via automation is a compelling part of a potential recovery scenario. This would be a platform in which you need a new "platform" to restore to but have good Veeam backup data. Consider some of these toolkits as opportunities to rapidly deploy in the event of a need for a complete recovery scenario.

Remediation

Despite all of the education and implementation techniques that are employed to be resilient against ransomware, organisations within the financial services sector should be still prepare for the worst-case scenario. At Veeam we have agreed upon 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 specifically what to do when a threat is discovered. Here are 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 fail over, 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 whole 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 anti-virus 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 financial services 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