Disaster Recovery: Mitigating Potential Cyberattacks

Ransomware attacks are unfortunately nothing new. These attacks involve taking over an enterprise's computer networks and present a growing problem which spans a diverse array of industries. Ransomware attacks are faced by organizations of all sizes.

Ransomware has been making headlines more recently, with an attack executed on US pharmaceutical giant ExecuPharm[1] who warned that Social Security numbers, financial information, driver licenses, passport numbers and other sensitive data has been accessed. Also, technology and consulting company Cognizant[2] was affected, and claims the attacks are causing service disruptions for many clients. Maze, DoppelPaymer and Sodinokibi are three ransomware groups to be aware of.

With the right knowledge and systems in place, including disaster recovery solutions, cyberattacks can be effectively mitigated, and companies and their customers can feel secure. Implementing disaster recovery measures are therefore critical to protect your business, customers and assets from the threat of ransomware.

Ransomware 101

Ransomware is a kind of malware from cryptovirology which threatens to publish the victim's data or consistently block access to this data unless a ransom is paid.

Ransomware is said to be the most lucrative form of malware in history[3], and attacks have only gotten worse, in both the number of occurrences and their complexity. Initially ransomware was used by hackers as a tool to extort money from individuals. It has evolved greatly to leverage complex tactics to compromise the data of large enterprises and threaten to sell it for a profit or post it publicly.

From start to finish, ransomware attacks can occur and aim to destroy anything from a partial to an entire business in a period of 15 minutes or less, making it difficult to mitigate once the attack is in effect.

Sources:

[1] Hackers publish ExecuPharm internal data after ransomware attack

[2] Cognizant confirms Maze ransomware attack, says customers face disruption

[3] Cisco 2016 Annual Security Report

Based on research of real-life global use cases, and experience, the process typically goes as such:

- Ransomware hackers gain access to a target network through phishing emails or other related means
- Employees click or open this malicious link and the ransomware begins to infiltrate the network and lock up files
- The ransomware targets backup files and folders, which prevents victims of having an 'out' as they become fully at risk of losing all of their data
- The files are encrypted and the ransomware executes an exchange with the server
- With no backup files to be accessed and encryption in place, the business is notified and a proposed ransom or threat is made with a specific time frame for adherence

While this occurrence sounds brutal, since ransomware is nothing new, there are many types of defense in place which have evolved to help organizations prepare and prevent them. Many human resources departments hold mandatory employee education sessions on cyberattacks and phishing emails to look out for. However, employees are human and the only way an organization can rest assured that its data is safe is to employ the right tools and systems to monitor, detect and prevent these attacks.

Making disaster recovery top of mind

Formerly, many companies rarely considered the true opportunities for catastrophic data loss to occur. They updated antivirus software programs or further secured firewalls. Now, with the spike in ransomware attacks, enterprises are completely rethinking their disaster recovery strategies.

With ransomware breaching IT systems more frequently than ever before, companies are labeling disaster recovery as a highly critical measure for the enterprise's health and security.
The global Disaster Recovery as a Service market is projected to grow at a CAGR of 27.81% to reach a value of $7.1 billion by 2025 from $1.6 billion in 2019.[4]

The healthcare, BFSI, IT and telecom industries are increasingly adopting data recovery as a service (DRaaS) solutions. Investing in secure data now translates to reduced operational costs, effective management of resources, reduced downtime and maximization of profits.[5] These investments are being made by companies of all sizes.

Sources:

[4] Global Disaster Recovery as a Service Market (2020 to 2025) - Featuring Veeam Software, Bluelock & Zerto Among Others

[5] Global Disaster Recovery as a Service Market (2020 to 2025) - Featuring Veeam Software, Bluelock & Zerto Among Others

The importance of awareness

Since ransomware is designed to be sneaky, it can go virtually undetected with too few security systems in place. Disaster recovery is focused on human awareness and protocols. For these reasons utilizing a cloud provider, whether cross, multi-cloud or hybrid cloud, for disaster recovery is so important. Even an enterprise's skilled IT professionals can easily miss ransomware warning signs.

Disaster recovery tools are designed to catch these attacks and alert businesses and stakeholders immediately.
The Disaster Recovery as a Service (DRaaS) market and available providers are also accurately aware of items to flag and prevent based on patterns and former occurrences.

The variety of options and partners available are therefore highly aware of how to enlist effective solutions and customize them to best handle a business's needs. These tools can be applied strategically based on enterprise size, end-user industry and geography to better account for individual requirements. Data backup versus enlisting full disaster recovery tools should no longer be a question in today's environment.

The benefits of cloud-based disaster recovery

Building a traditional disaster recovery center is one solution, but a trickier one for enterprises. They need to build or rent equipment rooms and invest significant manpower into maintenance and tests. If DR tests are performed in traditional DR centers, equipment rooms and cables must be scheduled and standby devices must be powered on, which often causes high fault rates. Accounting for all that is required, means incurring high CapEx and OpEx with the need for multiple centers to reach the same scale and provide real-time transmission.

Cloud disaster recovery utilizes one or multiple public clouds, including AWS, Azure or Google Cloud for example, to back up data and resources. Cloud-based partners are acutely aware of how to prevent cyberattacks. Then, if or when disaster occurs, an enterprise's resources can be restored from the cloud back to their original locations, either on-premise or in the cloud.

Cloud disaster recovery providers offer their users storage space and make regular updates to systems on which client-installed software is installed. Users can seamlessly add, change, manage and delete systems and storage capacity, without having to make long-term bets or consider back-end supported infrastructure.

Enterprises can benefit from cloud-based disaster recovery solutions to scale. These businesses are typically being billed monthly for the storage and the client software licenses.

Final takeaway

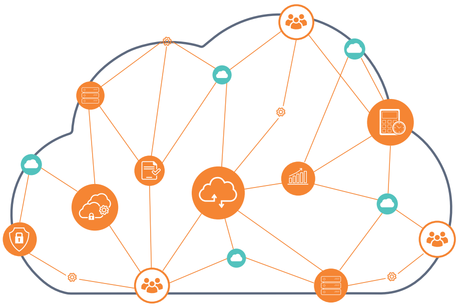
Regardless of your cloud strategy - multi-cloud or hybrid cloud - enlisting tools which assure you substantial disaster recovery methods for prevention is critical in today's climate. Some solutions offer faster Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) than others, so this is something to look out for. In general however, recovery from the cloud is quick since most cloud infrastructure provides high bandwidth and fast disk I/O.

The specific approach that your company enlists when designing its cloud disaster recovery architecture should of course depend on your needs and budget. Either way, you should be sure to recruit the services of a partner you can trust, such as Hystax OptScale to prepare you for these potential, and likely, ransomware attacks.

Cloud disaster recovery solutions provide necessary backup and recovery for critical server machines that host enterprise-level applications, such as MS-SQL, Oracle and others.

Hystax provides its users with seamless cloud migration and cross-cloud disaster recovery with RPO/RTO of seconds and minutes. It's key backup and disaster recovery capabilities provide background replication of business applications, machine data and metadata, automatically generated disaster recovery plans, restoration of all changes from disaster recovery sites back to production workloads within minutes and ensured economy on backup and disaster recovery overall.

About Hystax



Hystax, the leading MLOps and FinOps solution provider, develops its flagship product, OptScale, which allows running ML/AI or any type of workload with optimal performance and infrastructure cost by profiling ML jobs, running automated experiments, and analyzing cloud usage. Access to the OptScale open source solution is granted to users by the Apache 2.0 license. This enables Hystax to deliver the OptScale platform to a wider range of ML & Data engineers, cloud capacity managers, and FinOps enthusiasts.

The mission of Hystax is to help businesses optimize the performance and cost of ML model training jobs and increase the number of experiments an ML engineer can run.

The solutions of Hystax are currently the choice for such iconic brands as PwC, Ives Rocher, Nokia, DHL, and Airbus for its FinOps/MLOps adoption, offering them a platform that offers countless optimization recommendations and complete cloud cost visibility/control over Kubernetes, AWS, Microsoft Azure, Google Cloud Platform and Alibaba Cloud costs. The company was founded in 2016 and has customers in 48 countries.

Moreover, Hystax offers live cloud migration, cross-cloud disaster recovery, and cloud backup from an any-to-any cloud platform.

Our customers include:

AIRBUS pwc NOKIA YVES ROCHER DHL ·T··Systems·

Contact us for more information at **info@hystax.com**

+1 628 251-1280