THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22-Issue-37-December -2019

Avoid Data Lose by Maintaining Security Compliance and Business Continuity Plan

Rajeev Kanday* , Ashok Sharma**, Pranay Jha***

*Assistant Professor, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab
**Associate Professor, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab
***PhD Scholar, School of Computer Science and Engineering, LPU, Phagwara

Abstract

Security vulnerabilities and cyber-attacks are common issues these days despite having lot of security devices and policies in place. When any security breach occurs, this is always a priority to avoid the data lose as much as possible and recover it from ransomware attacks.

There are many solutions have already been implemented to detect and prevent security threats, but attackers always find a new gap to attack. There are certain approaches that are required and would not be needed for such attacks.

Managing the compliance and business continuity plan in terms of disaster recovery sites plays a vital role in such unforeseen issues. It outlines the policy and procedures to be carry out during any security threats in a Data Center. This will ascertain that Infrastructure is compliant which will reduce threats happen because of human error. Along with that, this will be able to provide the business user's access to the restored critical data of locally held systems.

Introduction

Compliance and Business continuity plans are most needed for an IT infrastructure. It plays a vital role in security the infrastructure. It outlines the policy and procedures to be carry out during any security threats in a Data Center. This will ascertain that Infrastructure is compliant which will reduce threats happen because of human error. Along with that, this will be able to provide the business user's access to the restored critical data of locally held systems [1].

Maintain Compliance

Maintaining compliance in an IT infrastructure is one of the major issues which needs attention by organizations. More than 30% of an IT budget spends on compliance and policies. If we maintain it properly, there are very less chances for attackers to find the gaps for any kind of security threat. Keeping an environment 100% compliance always provides secure and effective infrastructure as showing in figure 1.

Patch Management

Patch management consists security configuration management, vulnerability assessment, compliant analysis, and third-party end point protection. Patching certainly required for operating systems, virtual machines, and hardware whenever vendor release new patch. An IT administrator must take care of patch management without any avoidance [2].

Micro segmentation Protection

Compliance protection from upper layer to micro level exists at virtual network adapter is another point which avoid such threats by protecting at each layer [3].

Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-37-December -2019

Strict IAM Rules

Identity and Access Management should have evaluation policy so that if any employee leave the organization must not have access on any device. This is one of the major impacts for security threat by intentionally or unintentionally by human. Along with that, it is also recommended that access for the existing employees should also be in scan for any kind of unauthorized activity [4].

Maintain Documentation

Every work or change in an IT infrastructure must be documented with appropriate approvals. If someone is making any downtime or performing any activity on any virtual machine, it should follow proper Incident, Problem, or Change Management procedures. This will help to avoid threats as well as helps during the analysis of any reported security incident.



Figure 1: Compliance and Audit as a Security Avoidance

Reports & Auditing

IT administrators should maintain reports for each activity such as daily and monthly health check and auditing for the environment. Audit of each devices are also required to maintain the security of Datacenter [5].

Lifecycle Management

Proper recycling of old hardware and bring new hardware also makes lot of security boundary as old hardware doesn't have enhance capabilities to bout with latest security threats. Hence it is always recommended to run your Infrastructure on quite old physical servers. Same applies with software as well. Legacy software does not have proper patches to apply, which results to cause ineffective use of the software from security vulnerabilities [6].

Plan Disaster Recovery

Disaster Recovery Plan for Data Centre provides the key decision points, activities and actions required to restore critical, Global IT infrastructure operations and applications/services that may lose in the event of a foreseen or unforeseen disaster that disables all or part of the data lose in a Data Centre during security or ransomware attacks [7]. It is important for every organization to maintain the business continuity plan for numerous Application and Data Recovery Plans. Many of these Applications will require additional activities to recovery but an organization will be safe from data point of view. Business Continuity Plans are the responsibility of the business and should have implemented in each IT Infrastructure [8].

Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-37-December -2019

Depending on the circumstances and nature of the disaster event a decision will be made at the point of invocation whether to isolate the primary data center to prevent unpredictable system restarts and possible split-brain scenarios or whether to leave the primary site online.

In the event of an DR invocation the recovery software initiates tasks on both virtual machines and hypervisor in primary and recovery datacenter as well as the storage systems in both sites. By interfacing with the storage, recovery software instructs the storage RPA at recovery site to bring the replicated VMware LUNs online to specific recovery hosts in a write enabled state. Once presented, recovery software powers on the Virtual Machines and carries out network changes to assign an IP address for the recovery datacenter location. In effect the VMs are then live and working in recovery datacenter as opposed to primary datacenter [9].

There are numerous options available for disaster recovery.

Failover

This option could result in some lost data and may result in DR databases being a few minutes behind production. The data can be lost only if DR database does not have all the archives applied to it including current redo logs.

Role reversal

This option is used when it is a planned activity and both source and destination sites are available. In this case, switchover technology is used and there is no loss of data. After the role reversal reverse shipping of archives starts to keep earlier primary which is DR now remains in sync with new primary database.

Partial Catalog Replication

In this option, the entire image database from primary site is presented to recovery site continuously by integrating robocopy utility into a series of Windows batch scripts. With such continuous replication in place, it is possible to prepare recovery site target domain for recovery without import so that it can quickly be bought into operation when required.

Break Mirror

This removes the now Primary database from its partner making recovery site the Production site with DR exposed. Using this option, data lose is there, but impact will be less due to attacks as non-impacted site will start functioning with same copy of data.

Conclusion

After discussing of points in this paper, we came to conclusion that meeting compliance and availing Business Continuity Plan brings lot of security improvements in an IT infrastructure. Compliance provides avoidance of security threats by internal or external users either intentionally or unintentionally. At same time, business continuity plans facilitated failover to recovery site without impacting any other production data in case of security attacks. The VMs will get shut down at production environment and all data will be accessible through recovery site.

References

[1] Automatic Speech Recognition Systems for Regional Languages in India", *International Journal of Recent Technology and Engineering*, vol. 8, no. 23, pp. 585-592, 2019. Available: 10.35940/ijrte.b1108.0782s319.

 Copyright ⓒ 2019Authors

ISSN:0971-1260
Vol-22-Issue-37-December -2019

[2] Automatic Speech Recognition Systems for Regional Languages in India", *International Journal of Recent Technology and Engineering*, vol. 8, no. 23, pp. 585-592, 2019. Available: 10.35940/ijrte.b1108.0782s319.

[3] P. Jha and A. Sharma, "How can your IT Infrastructure Withstand the Pressure of Digitalization?", *International Journal of Research In Electronics And Computer Engineering*, vol. 7, no. 1, 2019. [Accessed 9 December 2019].

[4] P. Jha, R. Jha and A. Sharma, "Behaviour Analysis and Crime Prediction using Big data and Machine Learning", *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 1, pp. 461-468, 2019. Available: https://www.ijrte.org/wp-content/uploads/papers/v8i1/A3493058119.pdf. [Accessed 9 December 2019].

[5] P. Jha, S. Singh and A. Sharma, "Data Control in Public Cloud Computing: Issues and Challenges", *Recent Patents on Computer Science*, vol. 12, 2019. Available: 10.2174/2213275912666190617164550.

[6] P. Jha, S. Singh and A. Sharma, "Data Control in Public Cloud Computing: Issues and Challenges", *Recent Patents on Computer Science*, vol. 12, 2019. Available: 10.2174/2213275912666190617164550.

[7] A. Sharma, R.S. Thakur and S. Jaloree, “Investigation of Efficient Cryptic Algorithm for Image Files Encryption in Cloud”, International Journal of Scientific Research in Computer Science and Engineering, vol. 4, no. 5, pp. 5–11, 2016.

[8] A. Sharma, R.S. Thakur and S. Jaloree, “Investigation of Efficient Cryptic Algorithm for Cloud Storage”, in Fourth International Conference on Recent Trends in Communication and Computer Networks ComNet Narosa Publication, pp. 58–63, Nov 2016.

[9] A. Sharma, R.S. Thakur and S. Jaloree, “Investigation of Efficient Cryptic Algorithm for Video Files Encryption in Cloud”, International Journal of Scientific Research in Computer Science and Engineering, vol. 4, no. 6, pp. 8–14, 2016.

 Copyright ⓒ 2019Authors