ISSN No:-2456-2165

Organizational Cyber-Security Measures During COVID-19 Epidemic

Dr. Fernando Wangila, Ph.D.

Abstract:- The COVID-19 epidemic, from an organizational perspective, has created the need for organizations to introduce VDI systems that allows employees to work remotely in line with the requirements of government regulation to curb its spread. However, these new measures make the networks systems of organizations vulnerable top cyber attacks due to loopholes created the new remote access protocols. Therefore, it is important for entities to establish new cyber security measures that reduce the risk levels of the organizations. These include NSPs, Malware and Ransom protection software and Restricted Access user control systems. If organizations put in place these measures, they will help to ensure that they work efficiently with minimal risks to these attacks.

I. INTRODUCTION

The continuum of cybersecurity in the face of the COVID-19 epidemic has become a complex affair as organizations take radical measures to incorporate system upgrade to allow workers to operate from home. Unlike previously, when the majority of the organization safely operated their system only on-site, organizations must adopt remote access systems that give access to workers from their homes. Consequentially, this new dimensional change created to ensure business continuity introduces new cybersecurity risk given the reconfiguration of their mainframe system to allow increased traffic of remote access. Notably, these new adaptive measures create new loopholes- if organizations are not vigilant, that makes them vulnerable to cyber-attacks. In acknowledgment of this fact, it is imminent that organizations adopt prudent measures that increase risk management protocols against possible attacks. As such, entities must formulate risk management strategies that include but not limited to network security protocols, air-tight configuration systems, anti-malware preventive measures, and user access monitoring and incident control keys.

The organizational network change management approach must ensure that VDI procedural frameworks, either through cloud computing or software installed in the central network servers system, incorporate a minimal risk regime that helps to manage incident reports. The meaning of this approach is that before changes to the systems, the organization undertakes a pre-installation change assessment report that identifies the possible loopholes. Therein, constitute a management regime that helps to identify the procedural framework for response in case there is a breach in the system (Lee et al., 2016). Most of the VDI(Virtual Desktop Infrastructure systems can be customized to suit the level of access that each user gains depending on their clearance level within the company. The figure below shows how the system functions.

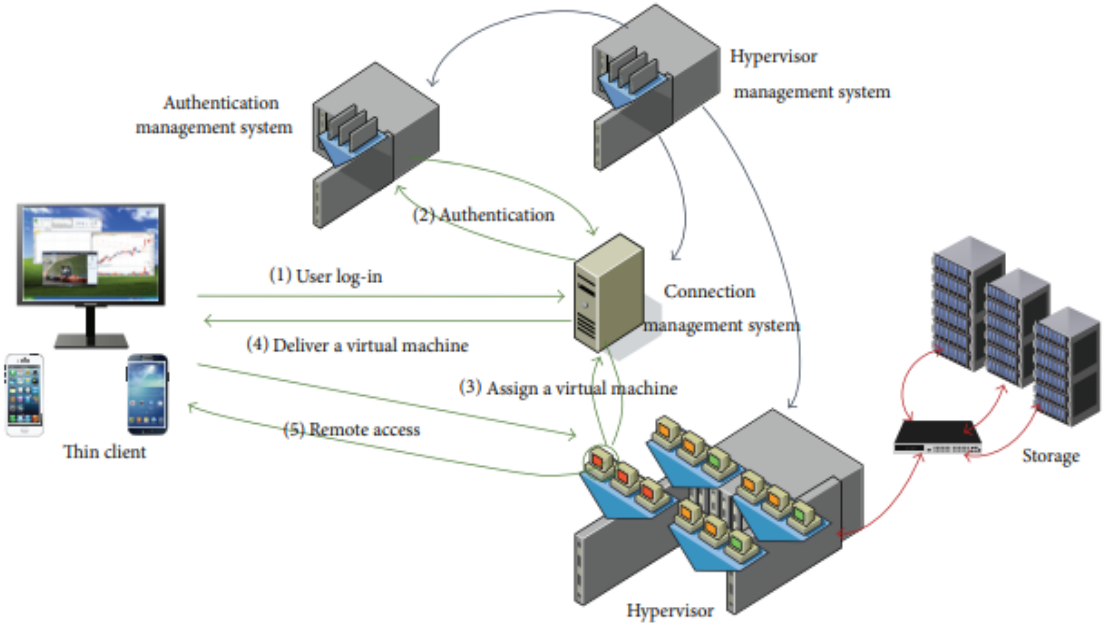

Fig 1:- Virtual Desktop Infrastructure for Remote Access of Employee during COVID-19 Lockdown

ISSN No:-2456-2165

As the figure above indicates, the RMR (Risk Management Regime) protocols may include an authentication management system and a hypervisor system that allows monitoring of the user activities. In case of any breach of unauthorized activity, the organizations may designate specific response mechanisms that may include immediate lockdown of the terminal where the breach occurs or depending on the level of attack initiate a complete lockdown that co0ntains the cyber attacks.

Of more importance for organizations to consider under the organization, changes in the secure configuration systems of all authorized personnel. The existing systems have unique approaches tailored to match the level of data sensitivity of an organization (Modelo-Howard et al., 2012). For example, for organizations in the banking systems, a breach may have very dire consequences not just for the organization but also for the customers; therefore, configurations may include regular sequential user access codes change through an automated system. In essence, the system automatically changes the access codes after a whole system review. Then, it sends the new codes to the employees through a secure network system connected to its central server system or the cloud computing systems for the remote access networks using internet-based communication systems between the organization's systems and employee devices.

Most of the cyber attacks that breach network systems mainly use malware and ransomware to create pathways that give them unauthorized access to the network system. As such, it will be necessary during the lockdown caused by the COVID-19 epidemic that the organization incorporates anti-malware prevention software systems that are updated continuously, not just for the central server network system but also for the user devices linked to the network that employees use to gain unprecedented access. In the past, most hackers have used employee devices as the weak-link through which they can gain access to the main organization's network systems. Therefore, the installation and updating of the anti-malware programs must be done both at the organizational server level and the remote user access device level (Lee et al., 2016). The two-tier system significantly boosts the security levels for organizations during the period when they must adapt to allow users unprecedented access to their central systems remotely to enable them to continue operations, albeit the high priority ones.

Virtual Desktop Infrastructure is not a new concept of the business world because e-activities that exist use a similar protocol. However, it becomes prudent that during this period, especially for the organizations that are expanding their access levels of remote access functionality they have stringent user interface monitoring system that not only allows prompt and effective response mechanisms but also manage the level of the privileges that remote access user enjoy when they are logged on in the system. This approach ensures that entities remain on high alert for possible cyber-attacks, and even when they happen, they contained within a very short period.

II. CONCLUSION

To conclude, the sustainability of the security paradigm for many organizations is dependent on the effective implementation of the measures that organizations take as they undertake the change during the COVID-19 lockdown period. Collectively, the proposed measures ensure that the VDI remote access protocols remain to serve the continued operational functionality of the organizations as opposed to security liabilities for the organizations. Indeed, the COVID-19 outbreaks come at a time when the world has advanced tech to ensure that all aspects of society continue to function despite the initiated lockdown.

REFERENCES

[1]. Lee, J. K., Moon, S. Y., & Park, J. H. (2016). CloudRPS: A cloud analysis based enhanced ransomware prevention system. *The Journal of Supercomputing*, *73*(7), 3065-3084. https://doi.org/10.1007/s11227-016-1825-5

[2]. Lee, K., Shin, J., Kwon, S., & Park, J. (2016). A study of the establishment of small and medium sized architectural design firm BIM environment based on virtual desktop infrastructure. *Korean Journal of Construction Engineering and Management*, *17*(5), 78-88. https://doi.org/10.6106/kjcem.2016.17.5.078

[3]. Modelo-Howard, G., Sweval, J., & Bagchi, S. (2012). Secure configuration of intrusion detection sensors for changing enterprise systems. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 39-58. https://doi.org/10.1007/978-3-642-31909-9_3