Datacenter Network Security

Name

Institutional Affiliation

Proposal overview

Technology has exponentially been growing over the last few decades. New technological capabilities and innovations have completely revolutionalised the information and technology sector. The growth of these new technologies and advancement in information technology has been accompanied by new threats to the security of the information infrastructure. Businesses have traditionally been guided by the idea of making profits which can only be arrived at through optimal operations. Optimal operation in this case means maximizing revenues while at the same time minimizing costs since profit is the difference between revenues and costs. Currently, businesses have become too dependent on technology especially information technology. Information plays a very key role in a business which has necessitated construction of data centers by nearly all business organizations. The businesses use these facilities to keep computer systems and components associated including information storage systems and telecommunications. Technically, data centers includes such components as data backup supplies, data connections and environmental controls such as air conditioning devices and fire suppression devices. Although businesses have excellently implemented data center requirements, they have specifically failed in one essential area which is the network security. The failure in implementing this particular area can be associated with business over emphasis on the bottom-line which is essentially profit making. Network security is an involving area which requires extra investment. The extra investment means additional costs which directly reduces business profits. For that reason, data centers have been finding it hard to keep with the demands associated with the appliances. Keeping up with the appliance demands which technically imply securing the data centers is one of the major problems business leaders across the globe are facing. Demand for information has both skyrocketed and become more dynamic in the current world of business. The growing demand of information has led to growth in the data market from 2009’s 108 million sq. ft. for example technology companies such as apple, Google and CISCO have supplied they customers with large number of devices which require data centers. On introduction of iPad, apple sold over 3.3 million units the first three months; Google activates over 100000 android-based smartphones on daily bases. Majority of customers across in addition to accessing application through VPN and wired networks, are accessing them through wireless and mobile networks. The users who use these devices and application expect high degree of convenience and consistency. The consistency and convenience can only be ensured if security is given the first priority by the data centers. Security has therefore grown to be a significant area of concern for data centers. Data centers support millions of sessions and connections flowing from all directions and therefore, if security of these sessions and connection is to be achieved, data centers play a monumental role. Information endpoints which have in current days been composed largely by mobile phones need to be protected from hackers. Corporate internal applications require to be protected from unauthorized access leading to phishing, data leakages, and hacking among other threats. SaaS require protection from password reuse, unauthorized access and level 7 attacks among other threats. it is therefore important that the data centers which are very important IT infrastructures, have sufficient mechanisms to uphold the convenient and consistency of use by the endpoint users.

To ensure that the data center technology fully protects endpoint users and itself from threats posed by cyber criminals and hackers, cloud-based security services have been launched as the formidable and sustainable solution. Cloud-based security has the ability to collect all anomalistic data throughout the internet and business networks using sensors. When such data is collected, it is analyzed so as to detect threat. On detection of threat, the cloud transmits the code to mitigate the threat. The codes or signatures mitigate the threat by updating the corporate IPSs.

Cloud based security services are easy to implement. Unlike other security features which include capital expenditure, cloud-based security services do not require capital expenditure. The firm which needs such services needs to approach the cloud-based services provide, agree on terms of business, that is, if the terms are to subscribe or to buy the services and immediately start using the services to both protect the data center and the endpoint users.

Literature review

Security of data centers has been researched and evaluated by several security professionals. Most of the professionals talk of the severity and dangers posed by the security threats posed by the security concerns. Others have gone ahead to propose solutions to these threats. I herein review four articles which expound on the data center security.

The first work to be reviewed is the work by Arista.com. (2013). The white paper acknowledges that security threats are more serious now more than ever before since they are stealthy and more targeted. The paper goes ahead to give examples of threats like APTs, DDoS attacks and complex multi-phase attacks which are so sophisticated that they are almost unable to be detected. Due to this, enterprises have the responsibility to ensure that their data centers are sufficiently equipped to protect themselves from the threats and dangers they pose. According to the paper, the best method in which an enterprise can protect itself is to ensure that it has in place active response plan and monitoring policy. The paper proposes that the most popular of methods to protect a data center is the use of cloud-based services. Many companies are doing this virtualizing their information resources to reduce the cost and increase agility. According to the paper, rethinking of security infrastructure in the data centers has been brought by the need to provide secure access, critical data protection, end user privacy protection and ensuring perpetuity of the business. These needs have even been increased by the increased demand of information services which are being provided by smartphones. The paper goes further to historically show just how costly threats can be. According to Arista.com, (2013), in 2013, cyber attacks led to 18% of data center outages. This was 16% increase from 2010’s 2%. As a result of advancement of commercially available attack tools and the increased cyber speed, the attacks have become more damaging and voluminous. Great number of dummy traffic is generated with short period of time and they often overwhelm in-line defense mechanisms. The paper then provides possible solutions to the problem. These solutions include network traffic monitors (data analytics, packet recorders, IPS, IDS and sniffers), active network scanners, in-line firewalls and gateways, and security information and event analytics (SIEMs).

The paper is of particular importance in my study because it affirms my proposition that the security concerns in data centers needs to be looked from another direction since they have evolved and advanced making it impossible for absolute security goals to be achieved.

The second article I have chosen to review is that by Trend micro, (2014). The paper acknowledges that virtualized systems are of great benefits to both the data center and the endpoint uses. It however warns that as one enjoys the benefits so derived, they should put measures in place to secure their virtualized data. Failure to take measure of protecting virtualized data centers will creates gaps which malicious individuals and hackers will optimally utilize the catastrophically cause damages to the organization. Putting these measures in place does not only protect the data centers but also ensures that the organization complies with privacy and security regulations. The paper proposes several cloud-based security solutions including deep security platforms, virtualization security, elastic cloud security, and web applications security. Several advantages of these cloud-based solution include prevention of data loses and disruption of business, reduction of operational costs, and ensuring cost effective compliance. The services work through detecting and shielding vulnerabilities, integrating detection and protection of the vulnerabilities to ensure maximum security, and ensuring unlimited SSL certificates.

The paper was chosen because it recognizes the problem and therefore proposes different ways of solving the problem. It enlists cloud-based as the best solution for ensuring security of the data centers. On top of this the paper also gives several examples of cloud based services which can be used to secure a particular data center. It goes on to positive feedbacks from several organizations which have successfully used the services. The aspects of the paper that makes it applicable in my research are that, just like the current paper, it affirms that there is a problem which threatens to compromise the security and privacy of information in the data centers. Like the current paper, the primary objective of the paper is to provide solution to the problem.

The third articles I will review is the article by Cohn, Deshpande, Kaushik, Mathews, & Nathan, (2013). Like the articles reviewed above, the article acknowledges that data centres have the responsibility of keeping information they deal with safe. It further adds that meeting the security goals has become complicated task due to the continued advancement which has allowed hackers and other malicious individuals to advance their ways. The security issues are further complicated by the fact that information demand has increased due to the incorporation of mobile devices in the corporate environment. The paper, due to these complications, condents that managing security concerns in the data centers is fixed, highly proprietary, expensive and complex adventure. The paper however reiterates the proposition of previous works that securing networks is critical part of business because it saves enterprises costs that would arise in cases when breaches are inevitable. The paper thus proposes Software-Defined Networking (SDN) as the best way to ensure that information system in the data centers and those that the data center controls are protected from potential threats. SDN provides the much needed flexibility in the data center. SDN has SDN controller which using the network analysis and statistics, manipulates the network path to provide open flow in a multi-tenant environment. Open flow is the first standard of SDN. The paper warn that despite the benefits derived from SDN, cloud, virtual environments and BYOD (Bring Your Own Device) poses new threats. Cohn, Deshpande, Kaushik, Mathews, & Nathan, (2013) advises that before deciding on security infrastructure to use, an enterprise should consider several factors including threats, performance, scale of operation and risk exposure among other factors.

The paper is relevant to my paper because in addition to illustrating possible threats and their causes, it presents potential solutions to the problem.

The fourth paper to be considered for review is by Anixter.com, (n.d.). The paper starts by acknowledging that cyber crime is rife and real. It gives an example of the recent credit card frauds which took the form of cyber crime. It further postulates that the consequences of data breaches have devastating effects to the relevant organization. The consequences in addition to the organization losing confidence of the people who had entrusted it with their data, has huge financial implications. The paper found that a single breach of information security cost a company average of $5.5 million. The primary causes of breaches according to the study are malicious attacks and negligent insiders. The paper is pessimistic in that it rules out the possibility of ever achieving absolutely secure cyber space. To that end therefore, the paper advises that it is imperative that every organization especially those that deal with sensitive data such as social security, healthcare and financial sector should make data center security a primary priority. The then gives the four layers of data center physical security. The four layers are the perimeter security, facility controls, computer room controls and cabinet controls. Addressing each of these layers according to the paper provides the firm with comprehensive protection of the data at risk of breach. The perimeter security aims at deterring, detecting and delaying threats. Such protecting includes perimeter fencing and infusing the perimeter fence with access controls, intrusion alarms, video surveillance and motion detection lighting. Facility controls aim at restricting access in case a breach occurs. This involves such things as indoor surveillance to identify and monitor whatever is taking place inside the data center. The computer room layer, through multiple surveillance, monitoring authorized access, verifications ensure that access is further restricted.

The paper is relevant to the current research as, unlike the other three papers, it gives physical precautions which should be taken to further ensure the data center is further secured.

Rationale of the problem

References

Arista.com. (2013). Security for the Cloud Data Center. Retrieved February 13, 2018, from [www.arista.com/assets/data/pdf/Whitepapers/ARISTA\_SecuritySolutionWP.pdf](http://www.arista.com/assets/data/pdf/Whitepapers/ARISTA_SecuritySolutionWP.pdf)

Trend micro. (2014). Cloud and Data Center Security. Retrieved February 13, 2018, from <http://apac.trendmicro.com/cloudcontent/apac/pdfs/business/sb01_clouddc_solution_140811us.pdf>

Cohn, M., Deshpande, S., Kaushik, M., Mathews, M., & Nathan, S. (2013, October 8). SDN Security Considerations in the Data Center. Retrieved February 13, 2018, from [www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf](http://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf)

Anixter.com. (n.d.). The Four Layers of Data Center Physical Security for a Comprehensive and Integrated Approach. Retrieved February 13, 2018, from [www.anixter.com/content/dam/Anixter/White%20Papers/12F0010X00-Four-Layers-Data-Center-Security-WP-EN-US.pdf](http://www.anixter.com/content/dam/Anixter/White%20Papers/12F0010X00-Four-Layers-Data-Center-Security-WP-EN-US.pdf)