New Challenges in Cloud, Demands New Solution

Jake Derkowski
Department of Computer Science
Cyber Forensics Intelligence Center
Sam Houston State University
Huntsville, TX, USA
jad084@shsu.edu

Cihan Varol
Department of Computer Science
Cyber Forensics Intelligence Center
Sam Houston State University
Huntsville, TX, USA
cxv007@shsu.edu

***Abstract*—It has been shown that the trajectory of technological innovation is pointing towards a world dominated by cloud computing. Recent events as well as new technologies have pushed everyone from small businesses to large corporations and most individuals to utilize its benefits–now the disadvantages need to be addressed more than ever. One of these disadvantages is the limited security that is currently provided by Cloud service providers (CSPs). The traditional security model seems to be an adequate solution for this new phenomenon, therefore a new solution is likely to be the best bet.**

In the aftermath of the COVID-19 pandemic, as well as the numerous other disasters the world has endured, some political scientists and other experts claim that war may be near, but it is even more likely that the next large war will take place in cyberspace. Now, as the number of companies in the cloud, they present an entirely new

attack vector that was once never possible, especially without ever coming face-to-face with them. We must come together to begin brainstorming ways in which we can protect our people, our economy, a

nd all other interests of ours in cyberspace. The purpose of this paper is to present a relatively new concept in network security called Zero Trust (ZT), to show how these concepts more closely align with the needs of cloud networks, and –most importantly– illustrate the Zero Trust Architecture (ZTA) in a

simple and inviting way such that the United States can be prepared for attacks; whenever they may come.

***Index Terms*—cyberspace, cyber warfare, cloud computing, cloud service providers, Zero Trust, traditional networking**

I. Introduction

[1]

Recent advancements in technology and current events, like the COVID-19 pandemic, has brought more attention to cloud computing for its versatility, it ' s availability, and scalability– all offered on a consumption-based cost model [2]. Cloud computing has taken away a lot of the responsibilities that all organizations must have had when using traditional networking. Instead, there are templates and containers that are out-of-the-box ready for development most of all the programming languages. This type of service is typically known as Software-as-a-Service (SaaS) and is the most common service for small businesses, those interested in migration and curious to try out the cloud. CSPs also offer infrastructure that is very customizable called platform-as-a-service (PaaS), examples may include SQL to NoSQL databases and operating systems. The last major type of cloud service is Infrastructure-as-a-Service (IaaS) which is most customizable allowing the customer to have full control over their hardware with having to be there physically to manage it. For all levels of responsibilities with their service types, the CSP will always be responsible for the management of the physical infrastructure, updating the hardware and software, and ensuring the highest level of availability that they can.

From an economic viewpoint, it is apparent why migration towards a cloud environment would be desirable because at baseline, utilizing the cloud frees up a lot of resources a lot of companies had to delegate to their on-premise network, which often was merely ro kept their systems online and functionable, but now this employees can return to the things the know the best–their company. This would ultimately drive more innovation and give organizations a better chance of fiscal success and triumph over the large supercorporations and thrive.

The COVID-19 pandemic has also been a driving force in the increased use and utilization of cloud computing because of the extremely quick change of work environment from on-campus networking to a remote desktop experience. Many organizations were not well equipped enough to perform this switch which resulted in a lot of organizations bankruptcy [2]. Even the organizations that did pursue to the end of the migration road and met the needs of a rapidly changing work environment were not necessarily out of water just yet. There has been a lot of speculation in the news and among academics that the rising tensions between the US and Russia may soon result in war [3], but it is more than likely going to be fought in cyberspace [4]. Therefore, it is important that we can quickly get some security in place before the attacks begin.

In this paper we will first look at related works on the types of security that the main CSPs deploy, then we will discuss our proposed solution, then we will look at some of the disadvantages or obstacles that this solution would have to overcome in the section; finally we will conclude with an analysis about they way we have addressed the problem.

II. Literature Review

When researching for articles related to security in the cloud or solutions to cloud weaknesses

during this research we noticed in [5], [6], [7] they all discussed the many benefits that the cloud offers but all of the articles we collected discussed their hear when it comes to the securing of the cloud. The articles [6] and [5] are still urging those organizations to begin the migration process but especially urge them to finish it. This is because a lot of these organizations which have a hybrid network have only added the vulnerabilities associated with the cloud to those that have been present for quite some time in the traditional model [8]. As for those who have already deployed their fully-cloud network they simply just had a change in their workplace–if anything.

Cloud service providers should do a better job at presenting their product in the way of the truth. There are countless videos illustrating the impeccable physical security of Microsoft and Google ' s datacenters, many of them I would bet were more secure than most military bases or buildings in the entire world–but this is not what is important to us–the cloud user. It is common knowledge that cyberattacks, as defined by [9] *is an act in cyber space that could reasonably be expected to cause harm*. This is what we are trying to explicate is that technology has now presented us with an entirely new domain in which wars can be fought. [9] continues by defining Cyber War as *...when a nation state declares war, and where only cyber warfare is used to fight this war*. This seems particularly unlikely to me that there were not any "boots-on-the-ground" whatsoever, but that could be due to numerous reasons.

However, [9] ' s definition begins to make more sense when we look back into history during the times of the cold war. The United States did not want to risk their lives to get to Russia just to be slaughtered when stationed at a bordering company; I assume likewise with Russia. But both parties fought each other in different ways such as the space race (which has become more popular recently) and performing suspicious fly-bys, anything possible to increase intimidation and fear in the opposition. We are seeing the sort of activities from both sides mentioned, plus malicious cyber activity from nations including China, North Korea, Iran, and Afghanistan [10], except these acts are not nearly as *innocent*. For an example, the war between Russia and Georgia in 2008 surrounding border disputes, Russia integrated cyber warfare into their political strategy by organizing a Distributed Denial of Service (DDoS) attack on key military sites and then coupled with attacks of local sites that were intended to cause civil panic and upheaval. At this point, all Russia had to do was to step in and take advantage of the chaos and assert their dominance [4]. This is one of many examples, but rest assured these the countries listed earlier have their own cyber war team, in the United States it is called the *US Cyber Command*.

war is coming [11] more war [3] **Comparing Security** [8] peacekeeping [5] CSP selection [7] Framework with Respect to Cyber Warfar [4] Forensics. nut wotn use [12]

III. Our proposal

It has been shown that it is great and even necessary for organizations to adapt with technology or they will face their demise. Unfortunately, new technologies have essentially put all an organization ' s information onto the world wide web and created a much larger attack surface–a surface that is not protected adequately by means of traditional network security. Instead a network that is built using Zero Trust principles moves aways from the border strengthening methods as we do in regular war and moves to secure one ' s resources by requiring authentication and authorization for each resource for the given network. This concept of *never trust, always verify* lays the foundation for all things Zero Trust [13].

NIST describes Zero trust as a *response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise owned network boundary* which focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource [13]. It is very possible that ZTA will one day become as standard as that cloud has, but we need to not make this a scary evolution. Cloud security providers need to step up and strengthen their own security by offering ways in which this integration can be made smoothly and perhaps in user-defined sizes.

Next we have provided a procedure that we recommend following to begin the process of designing future applications and for those that are already hosted on the cloud.

A. Build a Zero Trust Architecture

To build a ZTA, privileges need to be granted using the principle of least privilege as noted by [14]. This principle states that only the required access should be granted, access to resources that do not pertain to a given task should never be granted. This principle supports the "never trust" aspect of ZTA because if extra privileges are granted this implies that the organization *trusts* not to abuse it with malicious intent. This would render a network something other than ZTA. From the security viewpoint, it is always preferable for employees to ask for permission rather than beg for forgiveness later.

The success of ZTA implementation rests on the accuracy of the roles and groups that are created for the employees. These roles will determine the level of access granted to each type of position. This step, as crucial as it is, can be completed by nearly anyone–all that is required to to analyze job descriptions and make a diagram of the shared requirements of certain positions and those that are not shared. From this, someone in IT can easily determine the rights that each will require.

In this step, the authorization and authentication method should be agreed upon. There are many different options here, but there already exists tools that will make this decision relatively easy. We recommend that you use some variant of a NGFW because of their power to act as a PEP plus the ease of which it can be implemented. Specifically, Palo Alto's Next-Generation Firewall because it has built-in identity verification

that utilizes the ZT concepts. These include "User-ID", "App-ID", and "Content-ID" as filtering agents.

B. Create Policy

It is highly recommended to use the *Kipling Method* when creating ZTA policy because it enables the Application Layer security that must be present within a ZTA. This method uses the policy creation outline: "Who? What? When? Where? How? and Why?".

The more specific the rules are in the policy the more strict and secure the ZTA will be. This step, as the rest, will improve as iterations continue. These policies discussed below are arguably the most important to achieve Zero Trust.

- *Access Control Policy*–Once the roles have been defined, this is where the IT department will draft the corresponding access controls.
  In the spirit of ZTA–do not trust the IT department. Verify that you can fulfill your job requirements, report when you cannot. May this begin an organization-wide collaboration where not trust is likely to lead to strengthening department bonds and an organization [15].
- *Zero Trust Policy*–this is the policy which will allow the various network resources to communicate to one another and will specify the way in which it does. However intimidating this seems, creation of this policy can be viewed as nothing other than "connecting the dots"–dots is the work completed in the previous steps.

C. Monitor and Maintenance

The use of Next-Generation firewalls make all traffic visible, enabling for the monitoring and maintenance that is required for ZTA. Next-Generation firewall illuminate network traffic through, another built-in function, enabling micro-segmentation of perimeters. This will increase the logging potential and allow for dynamic policies to be made and distributed throughout the network. This is crucial, as well as one of the most desirable, aspects of the ZTA because it enables an organization's security to constantly improve and adapt to the ever changing workplace environment and IT landscape.

IV. Some Considerations

A lot of the time, organizations are reluctant to change rather it be because of the inability to see the need of staying as relevant as the technologies that they use or because the cost and fear of losing money when adjusting to new technology. The reason is not important here, but there are many more that make change difficult; just like during the COVID-19 pandemic, companies lost a lot of business because of their inability to change with the times which typically comes from the a lack of resources. This is our fear when it comes to promoting a new technology, especially when it is created from an entirely different philosophy as traditional network security did.

We have tried to present the idea of the Zero-Trust Architecture in a clear but pretty brief way because we do not want to scare away the people who would benefit from it the most. Fear not, just during timespan of this paper we have seen more and more integrations of the ZTA in all types of (unexpected) places–Microsoft Azure now has a Zero Trust compliance and integretion workbook.

V. Conclusion

It is more than apparent that technology is pushing more people to the cloud redistributing the hardware and software responsibility to the Cloud service providers. With our businesses living almost entirely online we must begin valuing the importance of good security. It is not a matter of if but it is a matter of when our weaknesses and vulnerabilities will be exploited–it is up to us now as business leaders, IT professionals, and employees in general to push ourselves and our colleagues to be open and willing to learn something new. We hope that this paper has provided the reader with some sense of confidence and motivation to be part of this innovation. If businesses, despite their industry could come together it would make this process much easier and ultimately create a much more secure cloud environment, one that is much more difficult to be penetrated by Russia and any other advisors.

References

[1] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in *2006 IEEE International Conference on Communications*, vol. 8, pp. 3383–3389, IEEE, 2006.

[2] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, p. 102248, 2021.

[3] Y. Raychev, "Cyberwar in russian and us military-political thought: A comparative view," *Information & Security: An International Journal*, vol. 43, pp. 349–361, 2019.

[4] P. Mali, J. Sodhi, T. Singh, and S. Bansal, "Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: An empirical study," *International Journal of Mechanical Engineering and Technology*, vol. 9, no. 2, 2018.

[5] M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," *International Journal of Information Management*, vol. 36, no. 4, pp. 618–625, 2016.

[6] V. Andrikopoulos, S. Strauch, and F. Leymann, "Decision support for application migration to the cloud: Challenges and vision," in *Proceedings of the 3rd International Conference on Cloud Computing and Service Science, CLOSER 2013, 8-10 May 2013, Aachen, Germany*, pp. 149–155, SciTePress, 2013.

[7] N. Ghosh, S. K. Ghosh, and S. K. Das, "Selcsp: A framework to facilitate selection of cloud service providers," *IEEE Transactions on Cloud Computing*, vol. 3, no. 1, pp. 66–79, 2015.

[8] S. Ristov, M. Gusev, and M. Kostoska, "A new methodology for security evaluation in cloud computing," in *2012 Proceedings of the 35th International Convention MIPRO*, pp. 1484–1489, IEEE, 2012.

[9] M. Robinson, K. Jones, H. Janicke, and L. Maglaras, "An introduction to cyber peacekeeping," *Journal of Network and Computer Applications*, vol. 114, pp. 70–87, 2018.

[10] S. J. Cimbala and R. N. McDermott, "A new cold war? missile defenses, nuclear arms reductions, and cyber war," *Comparative strategy*, vol. 34, no. 1, pp. 95–111, 2015.

[11] R. Haddick, "This week at war: Lessons from cyberwar i," *Foreign Policy*, vol. 28, 2011.

[12] A. Aminnezhad, A. Dehghantanha, M. T. Abdullah, and M. Damshenas, "Cloud forensics issues and opportunities," *International Journal of Information Processing and Management*, vol. 4, no. 4, p. 76, 2013.

[13] V. Stafford, "Zero trust architecture," *NIST Special Publication*, vol. 800, p. 207, 2020.

[14] I. Ahmed, T. Nahar, S. S. Urmi, and K. A. Taher, "Protection of sensitive data in zero trust model," in *Proceedings of the International Conference on Computing Advancements*, ICCA 2020, (New York, NY, USA), Association for Computing Machinery, 2020.

[15] B. Zimmer, "LISA: A practical zero trust architecture," in *Enigma 2018 (Enigma 2018)*, (Santa Clara, CA), USENIX Association, Jan. 2018.