Microsoft Azure Evolution, Benefits, and Challenges

Antonio Shields

School of Cybersecurity, Old Dominion University

CYSE 280: Windows Systems Management and Security

Prof. Malik A. Gladden

April 13, 2023

Cloud computing systems provide various services by means of the Internet. Some of the tools and applications the cloud computing systems can provide are storing data, software downloads and uploads, networking, remote servers, and database access from almost anywhere. Cloud computing can be utilized by individuals and by businesses either through a public cloud, a private cloud, or a hybrid cloud. With the internet's usability more popular than ever, there are many vendors now that offer cloud computing compared to 10 years ago. This paper will focus primarily on one of the cloud computing system offerings on the market, Microsoft Azure. The goal of this paper will be to provide background on Microsoft Azure from its inception to now, discuss some of Microsoft Azure's vulnerabilities they have encountered, and how Microsoft Azure compares to other cloud computing vendors on the market.

Windows Azure was initially announced on October 28, 2008, at the Professional Developers Conference that Microsoft held in Los Angeles, California. Windows Azure was introduced as a cloud computing operating system aimed to target Businesses and Developers without the need for additional coding, according to Abandy (2022). This Announcement came roughly two years after Amazon Web Services (AWS) launched its cloud service and was provided by Ray Ozzie, the chief software architect of Microsoft at the time. Windows Azure, according to Sleit et al (2013), "is an attempt to create an end-to-end cloud service offering in the platform, middleware, enterprise services, and consumer services categories." (p. 38). Windows Azure began with a limited number of services, which according to Abandy (2022) "enabled developers to run the ASP.NET web applications and API's, the other piece designed along with the Azure service was running long process with no User Interface (UI) for worker roles." (p. 1). According to Sleit et al (2013), Windows Azure, which is the cloud's operating system, SQL Azure, which is the database engine for the Azure platform, and AppFabric, formally known as the .NET Services, is the middleware component that contains ServiceBus and Access Control services, are the three main components. (p. 38). On February 1, 2010, Windows Azure became available commercially and was met with mixed reviews from analysts. Because AWS was out prior to Windows Azure's release for two years, AWS already had a foothold in the cloud computing market, resulting in Azure being compared to AWS's product offering. According to Harvey (2017), "Microsoft improved its product over time and added support for a wide variety of programming languages, frameworks, and operating systems, including Linux." (p. 1). Harvey (2017) also stated that "recognizing that its cloud computing service had moved far beyond Windows, the company renamed Windows Azure as Microsoft Azure in April 2014." (p. 1). Satya Nadella, who became Microsoft's chief operating officer in 2014 was influential in the name change from Windows Azure to Microsoft Azure because of wanting to expand to using open-source technology and companies outside of the Windows platform (Hyman, 2023). According to Hyman (2023), "Microsoft Azure provides first-class support for Linux-based VMs and non-Microsoft web applications and services."

There are three categories of cloud services that each vendor usually offers. Those categories are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). According to Alreshidi (2019), "IaaS is the delivery of complete computing infrastructure Over the Internet." (p. 165). Alreshidi (2019) also states that "IaaS is mainly for developers who want to develop their solutions on the top of the infrastructure and does not want to use any other of Cloud server providers tools or (Application Program Interface) APIs." (p. 165). IaaS gives most control and responsibility to the customers and developers and just using the cloud service for mainly hosting purposes of the servers and virtual machines. PaaS is, according to Luma-Osmani et al (2018), "a model where the service provider offers all the necessary tools and the hardware, it supports computing a platform which typically includes operating system, programming language, execution environment, database, web server." (p. 80). With PaaS, Azure would take more control of the application environment compared to IaaS, so that the customer and developers could focus on the applications and data management themselves. SaaS, according to Luma-Osmani et al (2018), "is a software distribution model in which a third-party provider hosts applications and makes them available to customers over a network, typically the Internet." (p. 80). An example of SaaS in the case of Microsoft Azure would be Office 365, where you can use Word, Excel, and Powerpoint through a web browser to create, edit, and save documents and access is maintained through multiple devices as long as the Office 365 account is logged into on those devices. Microsoft Azure offers all three services depending on a business's needs.

As previously mentioned, cloud computing has three different models: public cloud, private cloud, and hybrid cloud. According to Hyman (2023), "Microsoft Azure is a public cloud because its global data center fabric is accessible by the general public." Although it is considered a public cloud, there are multiple security layers used to ensure the privacy of data remains intact. Microsoft Azure also offers a private cloud option but can be very costly because of the private space requested. According to Hyman (2023), "typically only the largest enterprise organizations can afford having their own private cloud infrastructure with redundant data centers, storage, networking, and compute, but they may have security prohibitions against storing data in Microsoft's (or any other cloud provider's) physical data centers." The Hybrid cloud model is just a mix of using on-premise resources in combination with the cloud environment. According to Hyman (2023), "a hybrid cloud allows the business to salvage the on-premises infrastructure that it's already paid for while leveraging the hyper scale of the Azure public cloud.” Outside of these three cloud system models, Hyman (2023) mentions also that “Microsoft has three additional, separate Azure clouds for exclusive governmental use and restricted country usage.” Those cloud systems are not accessible by the general population and can only be accessed if affiliated with those entities.

Cloud computing’s responsibility for data storage on the Internet makes it a valuable resource for being able to access information anywhere, but that same accessibility also makes it a valuable target for threat actors looking to expose vulnerabilities and gain unauthorized access. Microsoft Azure utilizes many layers of security to maintain the privacy and protection of data, but it is not a stranger to vulnerability threats. A couple of vulnerabilities that have occurred in recent years have been to the Cosmos DB database and the Server-side request forgery attack. The Cosmos DB database vulnerability, according to Ricker (2021), “left more than 3,300 Azure customers open to complete unrestricted access by attackers.” (p. 1). Ricker (2021), states that “the vulnerability was introduced in 2019 when Microsoft added a data visualization feature called Jupyter Notebook to Cosmos DB.” (p. 1). Ricker (2021) also states that “the feature was turned on by default for all Cosmos DBs in February 2021.” (p. 1). Even though this was a major vulnerability, Microsoft reports that they did not see any activity or unauthorized data access from malicious actors attempting to exploit the vulnerability (Ricker, 2021, p. 1). The vulnerability was discovered by Wiz, which is a cloud security vendor and upon discovery, reported their finding to Microsoft and they were able to disable the vulnerability within 48 hours of being notified. (Ricker, 2021, p. 1). This vulnerability gave access to the primary keys that secured the database giving full read/write/delete access to whoever exploited the vulnerability. (Ricker, 2021, p. 1). Since Microsoft is unable to change the primary keys for the customers, they had to notify the affected customers of the vulnerability and instruct them to change their keys as a precaution. (Ricker, 2021, p. 1). Another vulnerability occurred between October 8, 2022 and December 2, 2022 and was discovered by Orca, another cloud security platform. According to Lakshmanan (2023), “Four different Microsoft Azure services have been found vulnerable to server-side request forgery (SSRF) attacks that could be exploited to gain unauthorized access to cloud resources.” (p. 1). The four attacks were as followed according to Lakshmanan (2023): “Unauthenticated SSRF on Azure Digital Twins Explorer via a flaw in the /proxy/blob endpoint that could be exploited to get a response from any service that’s suffixed with “blob.core.windows[.]net”, Unauthenticated SSRF on Azure Functions that could be exploited to enumerate local ports and access internal endpoints, Authenticated SSRF on Azure API Management service that could be exploited to list internal ports, including one associated with a source code management service that could then be used to access sensitive files, and Authenticated SSRF on Azure Machine Learning service via the /datacall/streamcontent endpoint that could be exploited to fetch content from arbitrary endpoints.” (p. 1). According to Lakshmanan (2023), “Three of the flaws are rated Important in severity, while the SSRF flaw impacting Azure Machine Learning is rated Low in severity.” (p. 1). All of the vulnerabilities, regardless of severity can be used for server manipulation to conduct attacks against other targets. (Lakshmanan, 2023, p. 1).

Azure cloud platform was introduced two years after AWS started its cloud service, so Azure was behind when it came to popularity in the market. Although Azure had a slow start, it has become one of the most used cloud services globally. According to Canalys.com (2023), “Microsoft Azure held 23% of the global cloud infrastructure services market and remained the second-largest provider after growing 31% year on year.” (p. 1). AWS comes in first place with 32% of the market share and Google Cloud comes in third place with 10% of the market but has had more growth at 36% yearly compared to both AWS and Azure. Some of the other cloud services in the market are the IBM Cloud, Rackspace, GoDaddy, 1&1 (which is now IONOS after merging), VMware, Red Hat, and Oracle Cloud. In comparing the top two, AWS and Microsoft Azure amongst each other, according to Madhuri and Sowjanya (2016), "AWS's Machines are individually accessible, Need proper mapping of internal machine names, domain names, and network file, Internal domain names automatically labeled as "local host" rather than individual machine domain name, EBS storage is sufficiently fast for big data, More mature environment for big data." (p. 3906). According to Madhuri and Sowjanya (2016), for Microsoft Azure, "Machines grouped into "cloud service" and respond to the same domain name but different ports, More memory allowance, Automation and user-friendly interface may be lacking, Less margin for error, Standard storage has difficulties for big data. Premium Storage (if available) is required, Less mature for big data, but improving." (p. 3906). Some of the advantages that Azure has over AWS according to Madhuri and Sowjanya (2016) is that "Amazon's Elastic Cloud Compute (EC2) is costlier than Azure, Azure has really zero maintenance, where you just implement your application and Microsoft will take care of your software, the maintenance cost is less compared to Amazon's EC2, and scalability is excellent in Azure." (pp. 3906-7).

Picking the right cloud computing platform for a business or individual ultimately comes down to their specific needs and budget. When cloud computing began over 10 years ago, the differences between each platform offering were drastically different, but as there are more technological advances, the differences are becoming minuscule and the decision of selecting a cloud service is becoming a matter of preference. All platforms have and will continue to be tested for vulnerabilities as long as there is information that belongs to others that can be acquired, so no platform is immune. Microsoft Azure, even though it had a late start, has proven to be a reliable cloud service that will continue to update and improve its offering to remain a leader in the cloud service industry.

References

Abandy, R. (2022, August 24). *The history of microsoft azure*. Techcommunity.Microsoft.com. Retrieved April 10, 2023, from https://techcommunity.microsoft.com/t5/educator-developer-blog/the-history-of-microsoft-azure/ba-p/3574204

Alreshidi, E. (2019). Comparative Review of Well-Known Cloud Service Providers (CSPS). *Science International*, *31*(1), 165–170. Retrieved April 10, 2023, from http://www.sci-int.com/pdf/636868844442264979.edited.pdf.

Canalys. (2023, February 8). *Worldwide Cloud service spend to grow by 23% in 2023* . Canalys Newsroom. Retrieved April 10, 2023, from https://www.canalys.com/newsroom/global-cloud-services-Q4-2022

Harvey, C. (2021, January 28). *What is Microsoft Azure Cloud & What is it used for?* Datamation. Retrieved April 10, 2023, from https://www.datamation.com/cloud/microsoft-azure-cloud/

Hyman, J. (2023). Chapter 1: Introducing Microsoft Azure. In *Microsoft Azure for dummies 2023*. essay, John Wiley & Sons Inc. Retrieved April 10, 2023, from https://learning.oreilly.com/library/view/microsoft-azure-for/9781119898061/c01.xhtml#h2-1.

Lakshmanan, R. (2023, January 19). *Microsoft Azure services flaws could've exposed cloud resources to unauthorized access*. The Hacker News. Retrieved April 10, 2023, from https://thehackernews.com/2023/01/microsoft-azure-services-flaws-couldve.html#:~:text=Four%20different%20Microsoft%20Azure%20services,unauthorized%20access%20to%20cloud%20resources.

Luma-Osmani, S., Idrizi, F., Ademi, S., & Fetai, R. (2018). Above the clouds: a brief overview of Microsoft Azure environments and applications. *Journal of Natural Sciences and Mathematics of UT*, *3*(5-6), 79–88. Retrieved April 10, 2023, from https://drive.google.com/open?id=1VSMA46-ZEFzdjvqhMSX2j3lijAY4oz5r.

Madhuri, T., & Sowjanya, P. (2016). Microsoft Azure v/s Amazon AWS Cloud Services: A Comparative Study. *International Journal of Innovative Research in Science, Engineering* *and Technology*, *5*(3), 3904–3908. Retrieved April 10, 2023, from http://www.ijirset.com/upload/2016/march/98_24_Microsoft.pdf.

Ricker, T. (2021, August 27). *Microsoft Azure Cloud Vulnerability is the 'worst you can imagine'*. The Verge. Retrieved April 10, 2023, from https://www.theverge.com/2021/8/27/22644161/microsoft-azure-database-vulnerabilty-chaosdb

Sleit, A., Misk, N., Badwan, F., & Khalil, T. (2013). Cloud computing challenges with emphasis on Amazon EC2 and windows azure. *International Journal of Computer Networks & Communications*, *5*(5), 35–44. https://doi.org/10.5121/ijcnc.2013.5503