Cloud Security Best Practices with Microsoft Azure

For the day 2 of cyber security caravan conducted by the Department of Information Communication Technology- Camarines Norte cluster on August 31, 2021, mr. Hermes Miraflor II, the guest speaker shared the Azure Platform, cloud foundations, cyber security on cloud, and monitoring, auditing and operations.

The topic introduces to us by showing first the key concepts and terms of cloud services. We leverage to internet today to share information and data using cloud computing. But, it doesn't mean we use the internet, it is already cloud computing. Cloud services should have the following characteristics to be considered one: it should have high availability, scalability, elasticity, agility, and it is fault tolerance. The different types of cloud models and services were also shared and explained to us. First type of cloud model is the *public cloud* wherein the service platform is owned by a certain cloud computing service provider, meaning it is a consumption-based model- you pay for what you will use and operate. This type of cloud model is accessed via secure network connection. The second model is private cloud wherein the platform is owned and operated by the organization that uses the cloud resources; this allows the organization to have complete control over their resources and security. This cloud model is created in the organization's data center, thus the organization is the one responsible for operating services they provide. The last model is the hybrid cloud, the combination of public and private cloud which gives flexibility to the organization. Besides the model, cloud has also different types of services. First is Infrastructure as a Service (IaaS) wherein the cloud consumer outsources the responsibility for the infrastructure to the cloud provider - the consumer will pay for the infrastructure, and the cloud service provider will provide depending on the consumer's payment. The next service is called Platform as a Service (PaaS) where it provides an environment for building, testing, and deploying software applications. The customer purchases or creates applications that are available on the internet along with its programming tools and languages required by the cloud. Then lastly is Software as a Service wherein users connect to and use cloud-based apps over the internet (Microsoft office 365 or calendar).

After the introduction of cloud, Azure is explained and discussed why security on the cloud. Azure is a hybrid cloud computing service by Microsoft. Azure provides different services like databases

(Azure SQL database, Azure Database for MySql, SQL server on virtual machine, and more). Azure also provides different platforms such as web and mobile development, containers, micro services, integration services, AI, and IoT. And these cloud services Azure provides will help in productivity of developers. Moreover, as cyber-attacks increase today and the global cost of cybercrimes keeps soaring. These hackers usually do the four phases of cloud kill chain model: First the exposure phase where hackers find vulnerabilities/loopholes to send malwares. The hackers will then access the environment and steal credentials or important data. And then once the hacker already is inside the network it is called the lateral movement phase, the hacker will snoop around to gather information, study the network traffic, and gain access to other databases inside the network. And the last phase is the action phase where the hacker can make use of the data he gathered by selling it to the black market for example. This is why cloud is recommended to use, because cloud providers will manage the security of the data center, however, it is emphasized that the security of cloud is always a partnership between the provider and user. And in Microsoft azure, they follow proactive approach for cloud security: migrate data to azure; securing environment; protect data by backing up data and disaster recovery; monitoring application, infrastructure, log analytics and diagnostics; configuring and automating to improve the azure deployments; then govern and establish best practices. In Microsoft Azure they also follow security posture: first detect fraud and abuse, auditing and certification, site penetration, and centralized logging and monitoring; second is to respond to those attacks; third is to protect the environment.

Lastly, mr. Miraflor provides a quick preview to show how to login to the azure portal, and access the virtual machine, with a process controller allowing only the owner to access that virtual machine.