T2022_23 Cloud computing and your organization (24th November 2022)

What is the cloud?

The cloud describes the software and databases that run on servers that may be accessed via the Internet. Data centers throughout the world house cloud servers. Users and businesses can avoid managing physical servers or running software on their own computers by utilizing cloud computing. Cloud-based services are now used by most, if not all, businesses, whether for storage, hosting software, or providing customer services.

How does cloud computing work?

Virtualization is a technique that makes cloud computing possible. By using virtualization, it is possible to create a simulated, digital-only "virtual" computer that functions just like a real one with its own hardware. Virtual machine is the technical word for such a computer. The files and apps from one virtual machine are not accessible to the other virtual machines, even though they are on the same physical computer, when virtual machines on the same host machine are properly configured, they are sandboxed from one another and do not communicate at all.

Additionally, virtual machines utilize the hardware that hosts them more effectively. One server becomes many servers by operating numerous virtual machines concurrently, and a data center multiplies into a plethora of other data centers that can accommodate numerous enterprises. As a result, cloud service providers may provide access to their servers to many more users simultaneously and at a lower cost than they could otherwise.

Cloud servers should always be online and accessible, even if some individual servers are down. Typically, cloud service providers back up their products across many machines and geographical locations. Regardless of the device they are using, users can access cloud services using a browser or an app by connecting to the cloud through the Internet, or through several interconnected networks. Thanks to cloud computing a user can log in to their Instagram account on a new phone after their old phone breaks and still find their old account in place, with all their photos, videos, and conversation history. It works the same way with cloud email providers like Gmail or Microsoft Office 365, and with cloud storage providers like Dropbox or Google Drive.

Models of Cloud Computing

Software-as-a-Service (SaaS): is where the software you would normally install on office computers is instead delivered via the internet. It is also commonly known as hosted software or hosted applications. Examples of SaaS applications include Salesforce, MailChimp, and Slack.

Infrastructure-as-a-service (IaaS): is where you rent space in a datacenter and use their servers rather than buying new hardware to run your business. A common example of IaaS is website hosting. IaaS providers include DigitalOcean, Google Compute Engine, and OpenStack.

Platform-as-a-Service (PaaS): In this model, companies don't pay for hosted applications; instead, they pay for the things they need to build their own applications. PaaS vendors offer everything necessary for building an application, including development tools, infrastructure, and operating systems, over the Internet. PaaS examples include Heroku and Microsoft Azure.

Risks of Cloud Computing

- Privileged user access- Keeping sensitive information with a third party has inherent risks because you are bypassing your company's own IT infrastructure and support team.
- Regulatory compliance- Customers are responsible for their own security and data integrity.
- Data location- You do not know where the information is physically being stored; it could be anywhere in the world.
- Data segregation- Your data is stored alongside other people's data and an encryption failure could make your data completely unusable.
- Recovery- What happens in a disaster? Is the data being replicated?
- Investigative support- Inappropriate or illegal activity might be hard or impossible to investigate.
- Long-term viability- What happens if your provider is bought out or bankrupt?
- Cyber Criminals- A malicious attack, such as a DDoS attack or a malware infection, cripples or destroys cloud infrastructure. An unauthorized user from outside the organization may also be able to access the data and expose or leak sensitive data.

Tips in choosing a cloud provider

Conduct a thorough analysis of the cloud provider market and only work with seasoned, resourceful businesses that enjoy a stellar reputation and, ideally, come highly recommended. They need to be able to assist you as your requirements change and your organization expands, comprehend your business model and

requirements, and be able to communicate with you in a manner that you can grasp. Your data will be housed in an environment that complies with worldwide baseline information security management standards of confidentiality, integrity, and availability if the provider has ISO 27001 accreditation.

Protecting your presence in the cloud

To guarantee data protection, integrity, and availability, you should take the following safeguards in addition to making an informed decision about your cloud provider:

- **Access Management**- Keep only those who absolutely require access to the cloud servers. Keep track of who has access to what data when and keep a clear audit trail of who has access to encryption keys (if used). If employees depart the company, change the encryption keys.
- **Encryption-** Make sure that any client data saved in the cloud is either encrypted or hashed to prevent unauthorized people from accessing it. When their cloud-based services were compromised, many major and small organizations were subject to legal prosecution for failing to appropriately protect data.
- **Firewall-** A cloud firewall provides a layer of protection around cloud assets by blocking malicious web traffic. Unlike traditional firewalls, which are hosted on-premises and defend the network perimeter, cloud firewalls are hosted in the cloud and form a virtual security barrier around cloud infrastructure.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

References

- Get Safe Online Guyana. *The Cloud*. Retrieved from Get Safe Online Guyana. https://www.getsafeonline.gy/business/articles/the-cloud/
- Cloud Flare. *What is the Cloud?* Retrieved from Cloud Flare. https://www.cloudflare.com/learning/cloud/what-is-the-cloud/