The emergence of cloud security

One of the most significant technology developments this century has been the emergence of cloud computing. The United Kingdom's National Cyber Security Centre defines cloud computing as, “An on-demand, massively scalable service, hosted on shared infrastructure, accessible via the internet.”

Earlier, you learned that most information is in the form of data, which is in a constant state of change. In recent years, businesses started moving their data to the cloud. The adoption of cloud-based services has complicated how information is kept safe online. In this reading, you’ll learn about these challenges and the opportunities they’ve created for security professionals.

A cloud lifting a business out of a marketplace and into the sky.

Soaring into the cloud

Starting an online business used to be a complicated and costly process. In years past, companies had to build and maintain their own internal solutions to operate in the digital marketplace. Now, it’s much easier for anyone to participate because of the cloud.

The availability of cloud technologies has drastically changed how businesses operate online. These new tools allow companies to scale and adapt quickly while also lowering their costs. Despite these benefits, the shift to cloud-based services has also introduced a range of new cybersecurity challenges that put assets at risk.

Cloud-based services

The term cloud-based services refers to a variety of on demand or web-based business solutions. Depending on a company’s needs and budget, services can range from website hosting, to application development environments, to entire back-end infrastructure.

There are three main categories of cloud-based services:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Software as a service (SaaS)

SaaS refers to front-end applications that users access via a web browser. The service providers host, manage, and maintain all of the back-end systems for those applications. Common examples of SaaS services include applications like Gmail™ email service, Slack, and Zoom software.

Platform as a service (PaaS)

PaaS refers to back-end application development tools that clients can access online. Developers use these resources to write code and build, manage, and deploy their own apps. Meanwhile, the cloud service providers host and maintain the back-end hardware and software that the apps use to operate. Some examples of PaaS services include Google App Engine™ platform, Heroku®, and VMware Cloud Foundry.

Infrastructure as a service (IaaS)

IaaS customers are given remote access to a range of back-end systems that are hosted by the cloud service provider. This includes data processing servers, storage, networking resources, and more. Resources are commonly licensed as needed, making it a cost-effective alternative to buying and maintaining on premises.

Cloud-based services allow companies to connect with their customers, employees, and business partners over the internet. Some of the largest organizations in the world offer cloud-based services:

- Google Cloud Platform
- Microsoft Azure

Cloud security

Shifting applications and infrastructure over to the cloud can make it easier to operate an online business. It can also complicate keeping data private and safe. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.

In a traditional model, organizations had their entire IT infrastructure on premises. Protecting those systems was entirely up to the internal security team in that environment. These responsibilities are not so clearly defined when part or all of an operational environment is in the cloud.

For example, a PaaS client pays to access the resources they need to build their applications. So, it is reasonable to expect them to be responsible for securing the apps they build. On the other hand, the responsibility for maintaining the security of the servers they are accessing should belong to the cloud service provider because there are other clients using the same systems.

In cloud security, this concept is known as the shared responsibility model. Clients are commonly responsible for securing anything that is directly within their control:

- Identity and access management
- Resource configuration
- Data handling

Note: The amount of responsibility that is delegated to a service provider varies depending on the service being used: SaaS, PaaS, and IaaS.

Cloud security challenges

All service providers do their best to deliver secure products to their customers. Much of their success depends on preventing breaches and how well they can protect sensitive information. However, since data is stored in the cloud and accessed over the internet, several challenges arise:

- **Misconfiguration** is one of the biggest concerns. Customers of cloud-based services are responsible for configuring their own security environment. Oftentimes, they use out-of-the-box configurations that fail to address their specific security objectives.
- **Cloud-native breaches** are more likely to occur due to misconfigured services.
- **Monitoring access might be difficult** depending on the client and level of service.
- **Meeting regulatory standards** is also a concern, particularly in industries that are required by law to follow specific requirements such as HIPAA, PCI DSS, and GDPR.

Many other challenges exist besides these. As more businesses adopt cloud-based services, there’s a growing need for cloud security professionals to meet a growing number of risks. Burning Glass, a leading labor market analytics firm, ranks cloud security among the most in-demand skills in cybersecurity

.

Key takeaways

So much of the global marketplace has shifted to cloud-based services. Cloud technology is still new, resulting in the emergence of new security models and a range of security challenges. And it’s likely that other concerns might arise as more businesses become reliant on the cloud. Being familiar with the cloud and the different services that are available is an important step towards supporting any organizations efforts to protect information online.

Resources for more information

Cloud security is one of the fastest growing subfields of cybersecurity. There are a variety of resources available online to learn more about this specialized topic.

- The U.K.’s National Cyber Security Centre
- has a detailed guide for choosing, using, and deploying cloud services securely based on the shared responsibility model.
- The Cloud Security Alliance®
- is an organization dedicated to creating secure cloud environments. They offer access to cloud security-specific research, certification, and products to users with a paid membership.
- CompTIA Cloud+

is a certificate program designed to teach you the foundational skills needed to become a cloud security specialist.

Revision #1
Created 17 July 2023 07:15:48 by naruzkurai
Updated 15 August 2023 18:44:10 by naruzkurai