Cloud Security

Contents

Overview

Cloud security sometimes referred as **Cloud computing security** is made up of *sets of policies*, *controls*, *procedures* and *technologies* that all work together for the purpose of protecting Cloud-based systems, infrastructure and data.

Configuration of these security measures is primarily for the purposes of:

- protecting data
- complying with regulations
- ensuring customer privacy
- enforcing authentication for individual devices or users

Cloud security is flexible and will support your business needs in most circumstances, such as:

- authentication
- traffic filtering
- firewalls

The configuration of security is done in one place.

This reduces the overhead for staff spending time on it, allowing for that extra time to be better spent in benefiting the business in other ways.

How Cloud security is delivered depends on both what it is being used to solve and which Cloud provider is used.

Additionally, it's not the sole responsibility of the business to implement it, but, instead, a joint effort between the business and the Cloud provider involved.

Why is Cloud security important?

With the current trend of businesses moving their services to the Cloud, robust security becomes imperative.

And while security measures are continually evolving, those that try to break down these measures don't stand still either.

As such, both sides are in a constant battle of attrition - constantly updating their security or anti-security techniques in an attempt to overwhelm each other.

It is important to consider that migrating to the Cloud *will not necessarily make your application more secure* than on-premises.

This is where security configuration comes into play - that will be what determines how secure your company will be from attacks.

These are the benefits that Cloud security offers:

- centralised security
- reduced costs
- reduced administration
- reliability

Centralised security

Moving your services to the Cloud centralises them, while at the same time security is also centralised into one place.

An on-premises network would have numerous devices and endpoints, and that still is the case even after migrating to the Cloud.

The bigger difference comes from it all being in one place, as it becomes a lot easier to analyse traffic and filtering.

Additionally, monitoring of networking and policy updates becomes a more streamlined process.

A big benefit is that you can configure your services for disaster recovery, as everything is in one place.

Cost-effectiveness

A big benefit of using Cloud storage and security services is that there is no big up-front cost for hardware.

This reduces capital expense at the same time reducing administrative overhead.

IT teams used to fight security issues reactively, once they appeared, whereas in the Cloud this fight happens far more proactively, before they appear.

The big payoff from this is that Cloud security is running 24/7 without any need for human intervention.

Reduced administration

Once your services are with a reputable Cloud provider, there will be no more manual security configurations or constant security updates.

These tasks are not only a massive time drain, but also places a big load on resources.

This is taken away once you move to the Cloud as all of the security is defined and controlled in one place.

Reliability

It wouldn't be an understatement to say that Cloud services provide the best dependability out there.

The only caveat to this is that the right security measures need to be in place and configured correctly for it to be effective.

Once that step is done, users can then safely have access to their data and applications in the Cloud.

Advantages

Businesses are noticing that moving their services to the Cloud gives them many benefits.

These benefits include things like:

- *scaling*
- *reduced costs*

- *using agile systems*

One thing businesses need to ensure is that they have complete confidence in the security that they implemented.

This generally means that the systems are secure from threats like:

- *data theft*
- *leakage*
- *deletion*
- *corruption*

Disadvantages

It doesn't matter whether you're using *Public*, *Private*, or *Hybrid* Cloud models, they are all susceptible to IT threads, mishandling, and human error.

That is why businesses are cautious of moving their systems to the Cloud.

However, given that the same threats can happen on on-premises infrastructure, everything boils down to how the security is implemented and managed.

Tutorial

This is a research-based Task.

Investigate what the most common security issues are for each of the : *Public*, *Private*, and *Hybrid* Cloud models.

Exercises

There are no exercises for this module.