Cloud Security Considerations

By Thomas M. Smith, CD, CISSP

March, 2022

ABSTRACT

Cloud services provide significant business opportunities, cost savings and increased visibility. Without careful planning, cloud services can pose significant risks to both a cloud service provider as well as a cloud customer. Unlike the traditional risks, each participant could isolate, contain and manage their security risks usually independent of each other. Then a cloud customer must trust that the cloud service provider is adequately managing its risks while adhering to the security practices that it claimed are in place and maintaining the controls that are mitigating security risks. This paper provides an overview of the cloud security considerations that a cloud customer should be aware of and create strategies to mange their security responsibilities.

Introduction

The National Institute for Standards and Technology (NIST) defines cloud computing as:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model is composed of five essential characteristics, three service models, and four deployment models."[1]

Service Overview

The standardized cloud-based service offerings are typically presented as:

- ***Software as a Service (SaaS):*** *The customer uses the applications made available by the service provider, which along with the accompanying Cloud Service Infrastructure are managed by the Cloud Service Provider and/or its subcontractor(s);*
- ***Platform as a Service (PaaS):*** *The customer deploys created or acquired applications, supported using languages, APIs, etc. within a Cloud Service Infrastructure supplied and managed by the Cloud Service Provider and/or its subcontractor(s); and*
- ***Infrastructure as a Service (IaaS):*** *The customer provisions, deploys, and manages system, network, and storage resources within a cloud service infrastructure supplied and managed by the service provider.*

Threat Environment

From a user perspective, threat actors include the non-malicious adversary (e.g., non-malicious unauthorized browsing, modification, or destruction of information due to the lack of training, concern, or attentiveness). These internal threat actors can create the conditions for a cyber-based attack or, in rare instances, be the attacker.

A more sophisticated threat actor is categorized as an Advanced Persistent Threat (APT). An APT as defined by NIST is: "*adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vector.*" [2] APTs have targeted cloud services in the past.

There are ample threats, vulnerabilities and other issues that need to be considered such as:

- **Data Breaches and Unauthorized Access:** Continued risk of unauthorized access to sensitive data stored in the cloud, leading to potential data breaches.

[1] NIST SP 800-145

[2] NIST Information Technology Laboratory: https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

Cloud Security Considerations

- **Misconfigured Cloud Settings:** Improperly configured cloud settings, especially in areas like storage buckets and security groups, that may expose sensitive data to unauthorized users.
- **Identity and Access Management (IAM) Challenges:** Issues related to inadequate management of user identities, permissions, and access controls, leading to unauthorized access.
- **API Security Concerns:** Vulnerabilities in cloud service interfaces and APIs, potentially exploited by attackers to gain unauthorized access or manipulate data.
- **Supply Chain Attacks:** Risks associated with third-party service providers and the potential for supply chain attacks that could impact the security of cloud services.
- **Advanced Persistent Threats (APTs):** Ongoing and sophisticated cyber threats targeting cloud environments with the aim of remaining undetected for extended periods.
- **Ransomware Targeting Cloud Assets:** A rise in ransomware attacks targeting cloud infrastructure and data, posing significant threats to data integrity and availability.
- **Zero-Day Exploits in Cloud Platforms:** The discovery and exploitation of previously unknown vulnerabilities in cloud platforms, potentially leading to security incidents.
- **Compliance and Legal Risks:** Challenges related to meeting regulatory compliance requirements and potential legal consequences associated with data stored in the cloud.
- **Insider Threats and Employee Negligence:** Risks associated with insider threats, whether intentional or unintentional, and the potential for employee negligence impacting cloud security.

While vendors may have addressed several of these issues, a customer should be aware of them and cross-reference their security practices to mitigation strategies.

Service Security Considerations

The availability of these types of cloud-based services is increasing as are the benefits that can be derived from using these services. From a security perspective, there are many questions that should be addressed and after an analysis of the results, the information should be provided to the business leaders and decision makers. Ideally the results of the analysis should identify the key security risks in a qualitative or quantitative format.

At a minimum, the information should outline the likelihood of a risk and the potential business impacts. Some of the information that is required scan be gathered from addressing security topics such as:

- Access management;
- Data ownership and geographical storage locations;
- Data comingling or separation;
- Disposal and retention of data;
- Disaster recovery and business continuity;
- Incident management;

- Monitoring service and performance levels;
- Service provider security and privacy policies and procedures
- Security controls to protect data in transit to/from the service provider location(s) (i.e. the cloud); and
- Security controls in place to protect sensitive data while at rest (i.e. data in storage).

Most smaller organizations that may benefit from cloud-based services may not necessarily be equipped to gather, analyze, and use the data that can be derived from these topics.

Typical cloud-based service providers have acknowledged that security is a shared responsibility. For example, the overall Microsoft security model is based on a shared responsibility where:

"*The Cloud Service Provider (CSP) is responsible for managing security and compliance of the cloud as the provider. The customer remains responsible for managing and configuring security and compliance in the cloud in accordance with their needs and risk tolerance*."[3]

Amazon Web Services has a shared responsibility model that states:[4]

> AWS Security Responsibilities
>
> *"Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is the number one priority of AWS."*
>
> *The Customer Security Responsibilities are:*
>
> *"With the AWS cloud, you can provision virtual servers, storage, databases, and desktops in minutes instead of weeks. You can also use cloud-based analytics and workflow tools to process your data as you need it, and then store it in your own data centers or in the cloud. The AWS services that you use determine how much configuration work you have to perform as part of your security responsibilities."*

Knowing this, customers should document their responsibilities and create strategies to implement, maintain and monitor security.

Security Principles Considerations

Customers should consider the following basic security principles and see how these can be applied to their intended service provider environment and who is responsible:

(1) ***Defence-in-depth:*** *technical, operational, and management security controls are used in a mutually supportive manner to mitigate risks.*

[3] As noted at: https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide.
[4] Amazon Web Services: Overview of Security Processes, March 2020.

(2) ***Least-privilege:*** users are provided the minimum access necessary to perform their duties.

(3) ***Prevent-detect-analyze-respond-recover (PDARR):*** *prevents attacks from being successful to through reasonable measures and ensure that successful attacks can be detected, contained, and damaged assets restored to a degree necessary to resume business.*

(4) ***Layered defence:*** *ensures that applications, databases, platforms, middleware, and communications are reasonably protected. A layered approach can effectively reduce the overall attack surface prevalent in a flat IT environment.*

Cloud service providers typically can address some of these principles by way of tenant protections as well as infrastructure and platform controls.

Customer considerations:

Customers should consult the vendor security and compliance information to better understand what they are recommending. For example, as part of the shared responsibility model, Microsoft recommends that the customer implement attack surface reduction rules that include preventing:

(1) All Office applications from creating child processes;

(2) Executable content from email client and webmail;

(3) Executable files from running unless they meet a prevalence, age, or trusted list criterion;

(4) Execution of potentially obfuscated scripts;

(5) JavaScript or VBScript from launching downloaded executable content;

(6) Office applications from creating executable content;

(7) Office applications from injecting code into other processes;

(8) Office communication application from creating child processes;

(9) Untrusted and unsigned processes that run from USB;

(10) Persistence through Windows Management Interface (WMI) event subscription;

Other security considerations:

- Review vendor security assessments and reports, most are made available to actual and potential customers.
- Review your organizations own security practices and seek improvements, especially incident management, data backups and policies.
- Document risks and develop a risk treatment plan.

Cloud Security Considerations

- Review Cloud service provider service level agreements to ensure they meet your business needs.

Summary

It is important for customers to identify and assess their security risks when considering cloud services. It is then necessary to understand whose responsibility it is to mitigate the various risks. The division of responsibilities and the implementation of the additional controls are an excellent approach to resolving security management expectations. Organizations would do well to document its own roles and responsibilities and create strategies to implement, monitor and improve security for the data in the cloud.

Bibliography

(1) Canadian Centre for Cyber Security, National Threat Assessment, 2021-2022.

(2) Canadian Centre for Cyber Security, Distributed denial of service attacks - prevention and preparation - ITSAP.80.110.

(3) Microsoft, Security and Information Protection for Multi-Region Organizations with a Single Microsoft 365 Tenant, March 2020.

(4) NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, Feb12, 2014.

(5) NIST, Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53, Revision 5, September 2020.