STC Cloud Services

Cloud Customers Cybersecurity Guide

Version: 1.0

Date: 02/11/2020

TABLE OF CONTENTS

1. Introduction to Cloud Computing Cybersecurity 3

2. Cloud Computing Cybersecurity Risks 4

2.1. Lack of the Cloud Cybersecurity Strategy and Architecture 4

2.2. Loss of Visibility 4

2.3. Insider Threats 4

2.4. Insecure Application Programming Interface (API) 4

2.5. Misconfiguration of the Cloud Services 5

2.6. Contractual Breaches 5

2.7. Compliance Violations 5

3. Cloud Service Customers Cybersecurity Responsibilities 6

3.1. Implement Strong Password Cybersecurity Policy 6

3.2. Deploy Multi-Factor Authentication (MFA) 6

3.3. Manage User Access 6

3.4. Perform Vulnerability and Penetration Testing 7

3.5. Implement Patch Management System 7

3.6. Monitor, Log, and Analyze User Activities 7

3.7. Secure User Endpoints 7

3.8. Implement Encryption 7

3.9. Applying Firewalls 8

3.10. Provide Cybersecurity Training 8

3.11. Create a Comprehensive Off-boarding Process 8

1. Introduction to Cloud Computing Cybersecurity

The Cloud Cybersecurity encompasses the technologies, controls, processes, and policies which combine to protect Customers Cloud-based systems, data, and infrastructure. It is a sub-domain of computer security and more broadly, information security.

It is a shared responsibility between stc and its Cloud Service Customers based on the Shared Security Responsibility Model (ref: Whitepaper-STC-Cloud-Shared-Security-Responsibility-Model). Further explanation of roles and responsibilities and services terms is available in the SLA document of each Cloud service, which is accessible through the Marketplace.

Customers shall implement the necessary Cloud Cybersecurity controls to protect the integrity and privacy of their virtual systems, data, and other virtual infrastructure and adhere to relevant regulatory compliance. Which in turn protects Customers from the reputational, financial, and legal ramifications of data breaches, data loss, and cyber incidents.

This whitepaper outlines basic Cybersecurity considerations in Cloud Computing to support Customers maturing the Cybersecurity practices. However, this document covers the minimum required Cybersecurity controls and it is the Customer's responsibility to understand their Cloud setup and implement all the required Cybersecurity controls.

2. Cloud Computing Cybersecurity Risks

Whether or not operating in the Cloud, Cybersecurity is a concern for all businesses. Customers face risks such as a denial of service, malware, SQL injection, data breaches, and data loss, which can significantly impact the reputation and bottom line of the business.

When Customers move to the Cloud, they introduce a new set of risks and change the nature of existing risks. That doesn't mean the Cloud computing is not secure. In fact, many Cloud Service Providers (CSPs) introduce access to highly sophisticated Cybersecurity tools and resources Customers couldn't otherwise access or use.

It simply means Customers need to be aware of the change in risks to mitigate them. So, let's take a look at the unique Cybersecurity risks of Cloud computing:

2.1. Lack of the Cloud Cybersecurity Strategy and Architecture

This is a risk that Customers can easily avoid. In their haste to migrate systems and data to the Cloud, many Customers become operational much before the Cybersecurity systems and strategies are in place to protect their infrastructure.

Make sure a Cybersecurity strategy is designed and implemented for the Cloud infrastructure, to go live in-line with their system migration plans.

2.2. Loss of Visibility

Customers often access a range of Cloud services through multiple devices, departments, and geographies. This kind of complexity, without the appropriate tools in place, can cause Customers to lose visibility of access to their cloud infrastructure.

Without the correct processes in place, Customers can lose sight of which team members are using the various subscribed Cloud services. Visibility is also scaring about what data the team members are accessing, uploading, and downloading. Eventually, leading to an increased risk of data mismanagement, potential breach, and data loss.

2.3. Insider Threats

Customers' employees, contractors, and business partners can be some of their biggest Cybersecurity risks. These insider threats don't need to have malicious intent to cause damage to the business. In fact, the majority of insider incidents stem from a lack of training or negligence.

2.4. Insecure Application Programming Interface (API)

When operating systems in the Cloud infrastructure, Customers might use an API to implement control. Any API built into the web or mobile applications can offer access internally by staff or externally by consumers.

External-facing APIs can introduce Cybersecurity risk, as an insecure external API becomes a gateway offering unauthorized access by cybercriminals looking to steal data and manipulate services.

2.5. Misconfiguration of the Cloud Services

With the increased range and complexity of services, managing and maintaining various configurations is a growing issue. Misconfiguration of Cloud services can cause data to be publicly exposed, manipulated, or even deleted.

Common causes include keeping default Cybersecurity, improper utilization of Cybersecurity groups, and access management settings..

2.6. Contractual Breaches

Contractual partnerships include restrictions on how any shared data is used, how it is stored, and who is authorized to access it. Customers' employees might unwittingly move restricted data into the Cloud service without authorization, leading to a breach of contract which could lead to legal action.

2.7. Compliance Violations

With the increase in regulatory control, Customers likely need to adhere to a range of stringent regulations & compliance requirements. When moving to the Cloud, Customers introduce the risk of compliance violations if they are not careful.

Many of these regulations require Customers to know where the data is, who has access to it, how it is processed, and how it is protected.

A careless transfer of data to the Cloud, or moving to the wrong Cloud provider, can put Customers in a state of non-compliance, introducing potentially serious legal and financial repercussions.

3. Cloud Service Customers Cybersecurity Responsibilities

Cybersecurity is a complex interaction of technologies, controls, processes, and policies. A practice that is highly personalized to Customers' unique business & technical requirements.

As such, there's no single explanation that encompasses how the Cybersecurity 'works'. However, there are widely established set of strategies and tools Customers can use to achieve a robust Cloud Cybersecurity setup, these include:

3.1. Implement Strong Password Cybersecurity Policy

Customers shall apply a minimum requirement on passwords such as all passwords should require one upper-case letter, one lower-case letter, one number, one symbol, and a minimum of 14 characters. Customers to enforce that users update their password every 90 days and set it so the system remembers the last 24 passwords.

A strong password Cybersecurity policy stops users from creating simple passwords, across multiple devices, and defend against most brute force attacks.

3.2. Deploy Multi-Factor Authentication (MFA)

Traditional username and password combinations are often insufficient to protect user accounts from hackers, and stolen credentials are one of the main ways hackers get access to Customers online business data.

Customers shall protect themselves with multi-factor authentication to ensure that only authorized personnel can log in to the Cloud accounts and services and access that sensitive data. MFA is one of the most effective ways of keeping would-be hackers from accessing Cloud services. MFA includes verifying the identity of the user by an additional medium such as One-Time Password SMS, Hardware Tokens, Authenticator Apps, etc.

3.3. Manage User Access

Customers shall have an Identity and Access Management (IAM) system to set proper levels of authorization to ensure that each employee can only view or manipulate the applications or data necessary for him or her to do their job.

Most employees don't need access to every application, every piece of information, or every file. Assigning user access rights not only helps prevent an employee from accidentally editing information that he or she isn't authorized to access but also gives protection from hackers who have stolen an employee's credentials. If an employee who has access to everything gets tricked by a phishing email and inadvertently provides their login information, all accessible data from that user's account will be compromised.

3.4. Perform Vulnerability and Penetration Testing

Customers shall practice Vulnerability and Penetration Testing by testing their Cloud infrastructure, to identify any potential weaknesses or exploits. Customers can then implement solutions to patch identified vulnerabilities to improve their Cybersecurity stance.

3.5. Implement Patch Management System

Customers shall implement an adequate level of the automated patch management system and establish the procedures and policies along with the implemented mechanism for patch management and vulnerability, making it certain that system, application, and network device vulnerabilities are properly evaluated.

Critical patches should be prioritized and vendor-supplied security patches should also be applied promptly for risk mitigation.

3.6. Monitor, Log, and Analyze User Activities

Customers shall implement real-time monitoring and analysis of user activities to spot irregularities that deviate from normal usage patterns, e.g., log in from a previously unknown IP or devices. These abnormal activities could indicate a possible breach in the system so catching them early on allows Customers to fix Cybersecurity issues before they can cause mayhem.

Various solutions can help Customers, starting with automated 24/7 networking monitoring and management and moving up to advanced cyber Cybersecurity solutions such as:

- Intrusion Detection & Response
- Vulnerability Scanning and Remediation
- Endpoint Detection and Response
- Security Information and Event Management (SIEM)

3.7. Secure User Endpoints

Customers shall introduce advanced client-side Cybersecurity to keep end-users' browsers up-to-date and protected from exploits as the majority of users access the Cloud services through web browsers.

Customers shall also implement an endpoint Cybersecurity solution to protect their end-user devices as most of the time, users access Cloud services through devices not owned by the Customers' company, such as mobile devices and other remote-working terminals/endpoints.

3.8. Implement Encryption

Customers shall implement encryption to protect their sensitive data, by encrypting them when at rest and in transit. This ensures that the encrypted data is near impossible to decipher without a decryption key that only the authorized recipient has access to.

3.9. Applying Firewalls

Customers shall protect their workloads using a traditional firewall and next-generation advanced firewall.

Traditional firewall protection includes packet filtering, stateful inspection, proxying, IP blocking, domain name blocking, and port blocking. Whereas, next-generation firewalls add a web application firewall (WAF), intrusion prevention system, deep packet inspection, application control, and analysis of encrypted traffic to provide comprehensive threat detection and prevention.

3.10. Provide Cybersecurity Training

Customers shall provide continuous Cybersecurity training to prevent employees from falling victims to social engineering breaches, such as leaking login credentials through phishing, spoofing websites, and social media spying. Training and awareness have to be done continuously periodically so that it becomes an effective preventive control.

3.11. Create a Comprehensive Off-boarding Process

Customers shall adopt a systemized de-provisioning process to ensure that access rights for each departing employee are revoked, and services are handed over to the respective service owner. This ensures that the departing employees can no longer access Company systems, data, customer information, and intellectual properties.