**Cloud Security Issues and Threats**

**Misconfiguration**

Misconfigurations of cloud security settings are a leading cause of cloud data breaches. Many organizations’ cloud security posture management strategies are inadequate for protecting their cloud-based infrastructure.

**Unauthorized Access**

Unlike an organization’s on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization’s cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization’s knowledge.

**Insecure Interfaces/APIs**

Cloud often provide a number of application programming interfaces (APIs) and interfaces for their customers. In general, these interfaces are well-documented in an attempt to make them easily-usable for customers.

**Hijacking of Accounts**

Many people have extremely weak password security, including password reuse and the use of weak passwords. This problem exacerbates the impact of phishing attacks and data breaches since it enables a single stolen password to be used on multiple different accounts.

Account hijacking is one of the more serious cloud security issues as organizations are increasingly reliant on cloud-based infrastructure and applications for core business functions. An attacker with an employee’s credentials can access sensitive data or functionality, and compromised customer credentials give full control over their online account. Additionally, in the cloud, organizations often lack the ability to identify and respond to these threats as effectively as for on-premises infrastructure.

**Lack of Visibility**

An organization’s cloud-based resources are located outside of the corporate network and run on infrastructure that the company does not own. As a result, many traditional tools for achieving network visibility are not effective for cloud environments, and some organizations lack cloud-focused security tools. This can limit an organization’s ability to monitor their cloud-based resources and protect them against attack.

**External Sharing of Data**

The cloud is designed to make data sharing easy. Many clouds provide the option to explicitly invite a collaborator via email or to share a link that enables anyone with the URL to access the shared resource.

While this easy data sharing is an asset, it can also be a major cloud security issue. The use of link-based sharing – a popular option since it is easier than explicitly inviting each intended collaborator – makes it difficult to control access to the shared resource. The shared link can be forwarded to someone else, stolen as part of a cyberattack, or guessed by a cybercriminal, providing unauthorized access to the shared resource. Additionally, link-based sharing makes it impossible to revoke access to only a single recipient of the shared link.

**Malicious Insiders**

Insider threats are a major security issue for any organization. A malicious insider already has authorized access to an organization’s network and some of the sensitive resources that it contains. Attempts to gain this level of access are what reveals most attackers to their target, making it hard for an unprepared organization to detect a malicious insider.

On the cloud, detection of a malicious insider is even more difficult. With cloud deployments, companies lack control over their underlying infrastructure, making many traditional security solutions less effective. This, along with the fact that cloud-based infrastructure is directly accessible from the public Internet and often suffers from security misconfigurations, makes it even more difficult to detect malicious insiders.

**Cyberattacks**

Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations’ cloud deployments are a common target of cyberattacks.

**Denial of Service Attacks**

The cloud is essential to many organizations’ ability to do business. They use the cloud to store business-critical data and to run important internal and customer-facing applications.

This means that a successful Denial of Service (DoS) attack against cloud infrastructure is likely to have a major impact on a number of different companies. As a result, DoS attacks where the attacker demands a ransom to stop the attack pose a significant threat to an organization’s cloud-based resources.

**Data Loss/Leakage**

Cloud-based environments make it easy to share the data stored within them. These environments are accessible directly from the public Internet and include the ability to share data easily with other parties via direct email invitations or by sharing a public link to the data.

The ease of data sharing in the cloud – while a major asset and key to collaboration in the cloud – creates serious concerns regarding data loss or leakage. In fact, 69% of organizations point to this as their greatest cloud security concern. Data sharing using public links or setting a cloud-based repository

to public makes it accessible to anyone with knowledge of the link, and tools exist specifically for searching the Internet for these unsecured cloud deployments.

**Data Residence/Control**

Most cloud providers have a number of geographically distributed data centers. This helps to improve the accessibility and performance of cloud-based resources and makes it easier for cloud to ensure that they are capable of maintaining service level agreements in the face of business-disrupting events such as natural disasters, power outages, etc.

**Cloud security solutions**

Organizations seeking cloud security solutions should consider the following criteria to solve the primary cloud security challenges of visibility and control over cloud data.

Visibility into cloud data — A complete view of cloud data requires direct access to the cloud service. Cloud security solutions accomplish this through an application programming interface (API) connection to the cloud service. With an API connection it is possible to view:

What data is stored in the cloud.

Who is using cloud data?

The roles of users with access to cloud data.

Who cloud users are sharing data with.

Where cloud data is located.

Where cloud data is being accessed and downloaded from, including from which device.

**Control over cloud data** — Once you have visibility into cloud data, apply the controls that best suit your organization. These controls include:

**Data classification** — Classify data on multiple levels, such as sensitive, regulated, or public, as it is created in the cloud. Once classified, data can be stopped from entering or leaving the cloud service.

**Data Loss Prevention (DLP)** — Implement a cloud DLP solution to protect data from unauthorized access and automatically disable access and transport of data when suspicious activity is detected.

**Collaboration controls** — Manage controls within the cloud service, such as downgrading file and folder permissions for specified users to editor or viewer, removing permissions, and revoking shared links.

**Encryption** — Cloud data encryption can be used to prevent unauthorized access to data, even if that data is ex-filtrated or stolen.

**Access to cloud data and applications**— As with in-house security, access control is a vital component of cloud security. Typical controls include:

**User access control** — Implement system and application access controls that ensure only authorized users access cloud data and applications. A Cloud Access Security Broker (CASB) can be used to enforce access controls

**Device access control** — Block access when a personal, unauthorized device tries to access cloud data.

**Malicious behavior identification** — Detect compromised accounts and insider threats with user behavior analytics (UBA) so that malicious data exfiltration does not occur.

**Malware prevention** — Prevent malware from entering cloud services using techniques such as file-scanning, application whitelisting, machine learning-based malware detection, and network traffic analysis.

**Privileged access** — Identify all possible forms of access that privileged accounts may have to your data and applications, and put in place controls to mitigate exposure.

**Compliance** — Existing compliance requirements and practices should be augmented to include data and applications residing in the cloud.

**Risk assessment** — Review and update risk assessments to include cloud services. Identify and address risk factors introduced by cloud environments and providers. Risk databases for cloud providers are available to expedite the assessment process.

**Compliance Assessments** — Review and update compliance assessments on cloud security standards.